МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет

КОМП’ЮТЕРНІ МЕРЕЖІ

Лабораторний практикум
для студентів спеціальності 123
«Комп’ютерна інженерія»

Київ 2021

УДК 004.7-0.57.175(076.5)
К637

Укладачі:
М.М. Проценко – канд. техн. Наук, доцент кафедри
Н.В. Пащенко – асистент кафедри

Рецензент *Є.І. Клюєв* – канд. техн. наук, доцент,
доцент кафедри інженерії програмного забезпечення
(Національний авіаційний університет)

Затверджено науково-методично-редакційною радою Національного авіаційного університету (протокол №4/21 від 14.05.2021 р.).

Комп'ютерні мережі : лабораторний практикум / уклад.:
К637 М.М. Проценко, Н.В. Пащенко. – К.: НАУ, 2021. 116 с.

Містить основні теоретичні відомості, практичні завдання до виконання лабораторної роботи, запитання до самоперевірки.

Для студентів спеціальності 123 «Комп'ютерна інженерія».

ЗМІСТ

ВСТУП

Лабораторний практикум «Комп'ютерні мережі» призначений для використання студентами, які навчаються за спеціальністю «Комп'ютерна інженерія» освітньо-професійної програми Бакалавр під час виконання лабораторних занять з однойменної дисципліни в навчальних лабораторіях університету. Практикум також слід використовувати під час проведення лабораторних занять зі студентами заочної форми навчання вказаної спеціальності.

Методичні розробки цього практикуму можуть бути корисними під час самостійного вивчення тематики комп'ютерних мереж в обсязі бакалаврської підготовки.

Матеріал лабораторного практикуму охоплює усі основні розділи дисципліни «Комп'ютерні мережі» бакалаврського рівня підготовки. У ньому розглядаються такі теми, як основи комп'ютерних мереж, у тому числі моделі мереж і засоби передачі мережевих даних, локальні та глобальні комп'ютерні мережі. Певна увага приділена комутованим мережам Ethernet, бездротовим і віртуальним мережам та іншим розділам, які стосуються нижніх рівнів моделі OSI.

Значна частина лабораторних робіт пов'язана з освоєнням технічних питань організації мережевого середовища для реалізації технологій протоколів TCP/IP.

Сюди відноситься IP-адресація, класова та безкласова адресація в мережах, робота з мережевими протоколами, такими як DHCP, HTCP, DNS, SMTP, POP3 та іншими. Також описана реалізація проблеми узгодження приватних та публічних IP-адрес в мережі Internet, робота зі списками.

Лабораторні завдання орієнтовані на виконання на програмному емуляторі комп'ютерних мереж Packet Tracer.

Цей пакет використовується провідною компанією з виробництва мережевого обладнання Cisco Inc. у своїй мережевій системі професійної освіти Cisco Academy як невід'ємний інструмент підготовки фахівців з мережевих технологій.

Лабораторна робота 1.
ОГЛЯД МЕРЕЖНИХ КОМПОНЕНТІВ. КАБЕЛЬНЕ ПЕРЕДАВАННЯ ДАНИХ

Мета: розглянути види та основні характеристики дротових ліній зв'язку.

Основні теоретичні відомості

Шлях, який проходить повідомлення від джерела до пункту призначення, може бути простим, наприклад, два комп'ютери з'єднані одним кабелем, або складним, наприклад, сукупність мереж, що охоплює земну кулю. Ця мережна інфраструктура забезпечує стабільний та надійний канал, по яким відбувається цей зв'язок.

Мережна інфраструктура містить три категорії мережних компонентів: пристроїв (обладнання), комунікаційних каналів та програмних компонентів (операційні системи, мережні служби та ін.).

Пристрої та комунікаційні канали – це фізичні елементи або апаратне забезпечення мережі. Апаратне забезпечення є видимими компонентами мережі: це ноутбук, ПК, комутатор, маршрутизатор, бездротова точка доступу або кабель, що використовується для підключення пристроїв.

Програмні компоненти включають багато поширених мережних додатків, якими користуються люди щодня, наприклад, послуги хостингу електронної пошти та послуги веб-хостингу. Мережні служби спрямовують та переміщують повідомлення через мережу. Програмне забезпечення для нас менш очевидне, але критичне для роботи мереж.

У даній лабораторній роботі розглянемо комунікаційні канали як компонент мережі.

Середовище передавання даних – сукупність ліній пересилання даних і блоків взаємодії (тобто мережного устаткування, що не входить до станції даних), призначених для пересилання даних між станціями даних. Середовища передавання даних можуть бути загального користування або виділеними для конкретного користувача.

Лінія передавання даних – це засоби, які використовуються в мережах для поширення сигналів у потрібному напрямі. Прикла-

дами ліній передавання даних є коаксіальний кабель, кручена пара проводів, світлопровід.

Канал зв'язку – це засоби одностороннього передавання даних. Прикладом каналу може бути смуга частот, виділена одному передавачу для радіозв'язку.

Дротовими лініями зв'язку є дроти без будь-яких ізолювальних або екрануючих опліток, прокладені між стовпами. Донедавна такі лінії зв'язку були основними для передавання телефонних або телеграфних сигналів. Сьогодні дротові лінії зв'язку швидко витісняються кабельними. Але подекуди вони все ще збереглися і за відсутності інших можливостей продовжують використовуватися також для передавання даних.

Кабельні лінії мають досить складну конструкцію. Кабель складається з провідників, укритий декількома шарами ізоляції: електричною, електромагнітною, механічною і, можливо, кліматичною. Крім того, кабель може бути оснащений рознімами, що дозволяють швидко приєднувати до нього різне устаткування.

Як середовище передавання інформації в мережах використовують три види кабелів: вита пара, коаксіальний кабель та оптоволоконний кабель (рис.1.1).

а) б) в)

Рис. 1.1. Види мережного кабелю:
а) вита пара б) коаксіальний кабель в) оптоволоконний кабель

Різні види мережних кабелів застосовуються в залежності від протоколів, розміру мережі та ін. У комп'ютерних мережах застосовуються кабелі, що задовольняють певним стандартам, що дозволяє будувати кабельну систему мережі з кабелів і сполучних пристроїв різних виробників.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вибрати варіант завдання з табл.1.1.
2. Вивчити теоретичну частину лабораторної роботи.
3. Ознайомитися з довідковою літературою.
4. Підготувати опис кабелю відповідно до варіанта завдання. Опис має містити:
   - вид кабелю та категорії;
   - історію створення та застосування;
   - схематичне позначення та принцип дії;
   - розніми та технічні характеристики;
   - переваги та недоліки.
5. Оформити звіт за результатами виконаної роботи.

Таблиця 1.1

Варіанти завдань

Номер варіанта	Вид мережного кабелю
1	вита пара екранована
2	коаксіальний кабель
3	оптоволоконний кабель
4	вита пара неекранована
5	«товстий» коаксіальний кабель
6	одномодовий оптоволоконний кабель
7	вита пара фольгована
8	«тонкий» коаксіальний кабель
9	багатомодовий оптоволоконний кабель
10	вита пара фольгована екранована

ІІІ. Запитання та завдання для самоперевірки

1. Які мережні компоненти ви знаєте?
2. Що таке середовище передавання даних?
3. Назвіть приклади ліній передавання даних.
4. Які види кабелів ви знаєте?
5. Наведіть відомі вам стандарти мережних кабелів.
6. Охарактеризуйте кабелі на основі витої пари.
7. Які джерела випромінювання застосовуються в оптоволоконних кабелях?
8. Опишіть основні типи й характеристики коаксіальних кабелів.

Лабораторна робота 2
ОГЛЯД МЕРЕЖНИХ КОМПОНЕНТІВ. БЕЗДРОТОВЕ ПЕРЕДАВАННЯ ДАНИХ

Мета: розглянути види та основні характеристики бездротових ліній зв'язку.

Основні теоретичні відомості

Бездротове передавання даних – це передавання даних без використання електричних провідників (дротів, кабелів) на певну відстань. Ця відстань може бути від кількох метрів до мільйонів кілометрів. Електромагнітні поля та хвилі найбільш цікаві з точки зору передавання комп'ютерних даних.

Якщо проаналізувати весь електромагнітний спектр, то можна прийти до висновку, що майже всі діапазони можна використовувати для передавання даних за допомогою амплітудної, частотної чи фазової модуляції хвиль.

Пристрої, спеціально призначені для випромінювання і (або) приймання електромагнітних хвиль, — це антени. Передавальні і приймальні антени мають властивість взаємності (оборотності), відповідно до якої одна і та сама антена може використовуватись як для випромінювання, так і для приймання електромагнітних хвиль. Якщо в електричний ланцюг включити антену відповідного розміру, то електромагнітні хвилі можна з успіхом приймати за допомогою приймача на деякій відстані. На цьому принципі засновані всі бездротові системи зв'язку.

Характеристики бездротової лінії зв'язку — відстань між вузлами, територія охоплення, швидкість передавання сигналів і т.п. — багато в чому залежать від частоти використовуваного електромагнітного спектра.

Для бездротового передавання даних можуть використовуватись радіохвилі, інфрачервоне та лазерне випромінювання, видиме або ультрафіолетове світло, мікрохвилі та ін.

Бездротові технології *Bluetooth* та *HIPERLAN* використовують смуги частот радіо- та ультракороткохвильового діапазону. Кожен радіомодем має антену та передавач для напрямленого передавання сигналів.

Що ж стосується технології *Wi-Fi*, то спочатку цей термін використовувався тороівельною маркою *Wi-Fi Alliance* тільки для позначення технології, що забезпечує зв'язок в діапазоні 2,4 ГГц і працює за стандартом *IEEE 802.11b*. Проте потім цим терміном все частіше стали називати й інші технології безпровідних локальних мереж. Будь-яке обладнання, яке відповідає стандарту *IEEE 802.11*, може пройти тестування в *Wi-Fi Alliance*; виробник цього обладнання за наявності позитивних результатів випробувань отримує відповідний сертифікат, а також право нанести логотип *Wi-Fi*.

Інфрачервоні бездротові мережі використовують для передавання даних інфрачервоні промені. У подібних системах необхідно генерувати дуже сильний сигнал, оскільки інакше значний вплив робитимуть інші джерела, наприклад світло з вікна. Цей спосіб дозволяє передавати сигнали з великою швидкістю, оскільки інфрачервоне світло має широкий діапазон частот. Для передавання даних використовуються три методи: сигнал може бути сфокусованим і спрямованим (пульт дистанційного керування телевізором), може випромінювати рівномірно у всіх напрямках; може відображатися від пофарбованих у світлий колір стель.

Подібним до інфрачервоного передавання даних є лазерний бездротовий зв’язок – необхідною є пряма видимість між передавачем і приймачем. Якщо з якої-небудь причини промінь буде перерваний, то перерветься і передавання даних.

Супутниковий зв’язок використовується для організації високошвидкісних мікрохвильових протяжних ліній. Оскільки для таких ліній зв’язку потрібна пряма видимість, яку внаслідок кривизни Землі неможливо забезпечити на великих відстанях, то супутник як відбивач сигналу є єдиним природним рішенням цієї проблеми. Технологія *VSAT* використовує для передавання даних геостаціонарні супутники, розміщені над екватором Землі на висоті 40 тис. км, супутники для системи *LEO* розміщуються набагато нижче – лише на висоті 100 км.

Ще одним популярним способом передавання даних є стільниковий зв’язок, який пройшов різні етапи розвитку (від *1G* до *5G*). Мережі на стільникових модемах працюють в особливо важких умовах великих завад, періодичного зникнення сигналу. Для передавання даних використовується аналоговий або цифровий сигнал.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вибрати варіант завдання в табл.2.1.
2. Вивчити теоретичну частину лабораторної роботи.
3. Ознайомитися з довідковою літературою.
4. Підготувати опис бездротової технології передавання даних відповідно до варіанта завдання. Опис має містити:
   - історію створення;
   - принцип роботи;
   - технічні характеристики;
   - застосування;
   - переваги та недоліки.
5. Оформити звіт за результатами виконаної роботи.

Таблиця 2.1

Варіанти завдань

Номер варіанта	Бездротова технологія або стандарт
1	*Bluetooth*
2	*Infrared Data Association*
3	*Worldwide Interoperability for Microwave Access*
4	*Z-wave*
5	*5G*
6	*Wi-Fi*
7	*Circuit Switched Data*
8	*Very Small Aperture Terminal*
9	*CDMA*
10	*ZigBee*

Запитання та завдання для самоперевірки

1. Поясніть відмінність між кабельним передаванням даних і бездротовим.
2. Який основний принцип бездротових систем зв’язку?
3. Яке середовище використовується під час бездротового передавання даних?
4. Назвіть основні характеристики бездротового зв’язку.
5. Назвіть основні технології бездротового зв’язку.
6. Яке середовище може бути використанедля бездротового передавання даних?

Лабораторна робота 3
МОДЕЛЬ OSI

Мета: проаналізувати рівні еталонної моделі *OSI*.

Основні теоретичні відомості

Еталонна модель *OSI (The Open Systems Interconnection model)* є визначальним документом концепції розробки відкритих стандартів для організації з'єднання систем. Відкрита система – це система, доступна для взаємодії з іншими системами відповідно до прийнятих стандартів.

Модель *OSI* була розроблена з метою спрощення взаємодії пристроїв в мережах і є рекомендаціями розробникам мереж і протоколів для побудови стандартів сумісних мережних програмних продуктів. Вона визначає сім рівнів взаємодії систем в мережах з комунікацією пакетів, дає їм стандартні імена і вказує, які функції повинен виконувати кожний рівень. Під час розробки моделі виділення рівнів базувалося на наступних принципах:

– кожний рівень повинен виконувати окрему функцію;

– потік інформації між рівнями повинен бути мінімізований;

– функції рівнів повинні бути зручні для визначення міжнародних стандартів;

– кількість рівнів повинна бути достатньою для поділу функцій, але не надлишковою.

Виділяють наступні рівні *OSI* (табл.3.1).

Таблиця 3.1

Рівні моделі OSI

Дані	7 прикладний ***application***	Доступ до мережних служб
	6 представлення ***presentation***	Представлення і кодування даних
	5 сеансовий ***session***	Управління сеансом зв'язку
Сегменти	4 транспортний ***transport***	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережний ***network***	Визначення маршруту і логічна адресація
Кадри	2 канальний ***data link***	Фізична адресація
Біти	1 фізичний ***physical***	Робота із середовищем передавання, сигналами і двійковими даними

Фізичний рівень призначений безпосередньо для передавання потоку даних. Здійснює передавання електричних або оптичних сигналів у кабель і відповідно їхній прийом та перетворення в біти даних відповідно до методів кодування цифрових сигналів.

Канальний рівень перевіряє доступність середовища передавання, реалізує механізми виявлення і корекції помилок, забезпечує коректність передавання кожного кадру (групи бітів).

Мережний рівень призначений для визначення шляху передавання даних. Відповідає за трансляцію логічних адрес й імен у фізичні, визначення найкоротших маршрутів, комутацію й маршрутизацію пакетів, відстеження неполадок і заторів у мережі.

Транспортний рівень призначений для доставки даних без помилок, втрат і дублювання в тій послідовності, як вони були передані. При цьому неважливо, які дані передаються, звідки й куди, тобто він надає сам механізм передавання.

Сеансовий рівень координує взаємодію користувачів, що встановлюють зв'язок, відповідає за підтримку сеансу зв'язку, дозволяючи додаткам взаємодіяти між собою тривалий час.

Рівень ***представлення*** має справу із синтаксисом і семантикою переданої інформації, тобто тут встановлюється взаєморозуміння двох сполучених комп'ютерів відносно того, як вони представляють і розуміють після одержання передану інформацію.

Прикладний рівень забезпечує взаємодію мережі й користувача. На цьому рівні реалізуються передавання файлів, віддалений термінальний доступ, електронне передавання повідомлень, керування мережею та ін.

Комп'ютерні мережі складаються з різного устаткування різних виробників, і без прийняття всіма виробниками загальноприйнятих правил побудови персональних комп'ютерів і мережного устаткування, забезпечити нормальне функціонування мереж було б неможливим. Тобто необхідний єдиний уніфікований стандарт, який визначав би алгоритм передавання інформації в мережах. В сучасних обчислювальних мережах роль такого стандарту виконують мережні протоколи.

Взаємодія однойменних функціональних рівнів по горизонталі здійснюється за допомогою протоколів. Протоколом називається набір правил і методів взаємодії однойменних функціональних рівнів об'єктів мережного обміну.

Взаємодія функціональних рівнів по вертикалі здійснюється через інтерфейси. Інтерфейс визначає набір функцій, які нижчий рівень надає вищому рівню.

Семирівнева модель *OSI* є теоретичною і містить ряд недоліків. Реальні мережні протоколи змушені відхилятися від цієї моделі, забезпечуючи можливості, які не було передбачено. Тому прив'язка якихось із них до рівнів *OSI* є дещо умовною.

Чітке визначення інтерфейсів за рівнями дозволяє заміняти один протокол рівня на інший без зміни стандартів протоколів суміжних рівнів. У цьому полягає основна цінність моделі *OSI*.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Заповнити табл. 3.2, вписавши в кожному рядку протоколи, технології та пристрої, які відповідають кожному рівню моделі *OSI*.
4. Оформити звіт за результатами виконої роботи.

Таблиця 3.2

Завдання

Рівень моделі *OSI*	Протоколи та технології	Пристрої
1 Фізичний		
2 Канальний		
3 Мережний		
4 Транспортний		
5 Сеансовий		
6 Представлення		
7 Прикладний		

Запитання та завдання для самоперевірки

1. Що таке протокол та інтерфейс?
2. Що таке відкрита система?
3. Назвіть рівні моделі *OSI*.
4. Об'єкти якого рівня моделі *OSI* забезпечують передавання даних від джерела до приймача?
5. Які функції виконуються об'єктами рівня представлення?

Лабораторна робота 4
ETHERNET ТЕХНОЛОГІЇ ЛОКАЛЬНИХ МЕРЕЖ

Мета: дослідити принципи побудови та функціонування мереж типу *Ethernet*.

Основні теоретичні відомості

У сучасних комп'ютерних мережах формування кадрів та передавання даних каналами зв'язку регламентується технологією *Ethernet*. *Ethernet* – сукупність технологій пакетного передавання даних, протокол кабельних комп'ютерних мереж, що працює на фізичному та канальному рівні мережної моделі *OSI*. Ця група мережних технологій регламентується стандартами *IEEE802.2 і 802.3*.

Систему *Ethernet* складають три основні елементи:

- фізичне середовище, яке використовується для перенесення сигналів *Ethernet* між комп'ютерами;
- пакет *Ethernet*, який складається із стандартизованої системи бітів, що використовується для перенесення даних через систему;
- правила доступу до середовища, вбудовані в кожний інтерфейс *Ethernet*, що дозволяє багатьом комп'ютерам коректно здобувати доступ до спільних каналів *Ethernet*.

Локальні мережі *Ethernet* використовують широкомовну мережну топологію, тобто сигнал, який передається довільною станцією, досягає до всіх інших станцій в мережі. Щоб вислати дані, станція спочатку прослухує канал, і коли канал простоює, станція висилає свої дані, упаковані у вигляді пакета *Ethernet*.

Для будь-якого обміну даними необхідний спосіб ідентифікації відправника та отримувача. У мережі *Ethernet* у кожного підключеного вузла існує фізична адреса, яку називають адресою управління доступом до середовища або *MAC*-адресою. *MAC*-адреси присвоюють в процесі виробництва всім мережним інтерфейсам *Ethernet*.

Перший елемент в умовному позначенні *Ethernet* – швидкість передавання в Мбіт/с; другий елемент позначає спосіб передавання: *Base* – пряме немодульоване передавання, *Broad* – використання широкосмугового кабелю з частотним ущільненням каналів; третій елемент – середовище передавання (*T*– вита пара, *F*– оптоволокно) або довжина сегмента кабелю в сотнях метрів.

Так, наприклад, позначення *10Base-T* означає швидкість передавання даних 10 Мбіт/с, пряме немодульоване передавання, вита пара.

Існує декілька форматів *Ethernet*-пакета – первинний *Version I* більше не застосовується; *Ethernet II* або *DIX* або 802.2 є найпоширенішим; *Novell* – внутрішня модифікація *IEEE 802.3* без *LLC; IEEE 802.2 LLC; IEEE 802.2 LLC/SNAP*. Структура пакета *Ethernet II* показана у табл. 4.1.

Таблиця 4.1

Структура пакета *Ethernet II*

DA	***SA***	***T***	***Дані***	***FCS***
MAC-адреса відправника	*MAC*-адреса одержувача	умовний тип протоколу	Дані, що пересилаються	Поле контрольної суми
6 байтів	6 байтів	2 байти	56-1500 байтів	4 байти

Пакет також містить поля «Преамбула» 7 байтів та «Ознака початку кадра» 1 байт. Ці поля не приймаються до уваги під час обчислення довжини кадра.

Формат пакета *Ethernet 802.2* має деякі недоліки, наприклад, він має парну кількість байтів службової інформації, що є не дуже зручно для роботи більшості мережних пристроїв.

Існують ще три стандарти формату кадру *Ethernet*:

− кадр *802.3/LLC* є стандартом комітету *IEEE 802* і побудований відповідно з прийнятим розбиттям функцій канального рівня на рівень *MAC* і *LLC*;

− кадр *Raw 802.3* або *Novell 802.3* з'явився в результаті зусиль компанії *Novell* з прискорення розробки свого стека протоколів в мережах *Ethernet*;

− кадр *Ethernet SNAP* став результатом діяльності комітету 802.2 з приведення попередніх форматів кадрів до деякого загального стандарту й надання кадру необхідної гнучкості для обліку в майбутньому можливостей додавання полів або зміни їх призначення.

Варто зазначити, що кадри останніх трьох форматів фактично не використовуються сьогодні, унаслідок більш складного формату, який виявився непотрібним в умовах існування єдиної технології канального рівня.

Формат пакета *Ethernet* ідентичний для всіх варіантів середовищ (кабельних систем) *Ethernet*, однак варіанти мереж *Ethernet*

для швидкостей передавання 10 Мб/с, 100 Мб/с, 1 Гбіт/с та 10Гбіт/с застосовують відмінні кабельні системи, різні компоненти і мають різні правила конфігурації.

Стандарти і технологія переносяться на специфічні продукти, які використовуються для побудови мережі *Ethernet*. Карта мережного інтерфейсу (*Network Interface Card - NIC*), яку також називають мережним адаптером або мережною картою – це пристрій, який здійснює фізичне під'єднання комп'ютера до мережі, тобто забезпечує фізичне сполучення між мережним кабелем і внутрішньою шиною комп'ютера. Кожен мережний пристрій має унікальну *MAC*-адресу. Оригінальна *MAC*-адреса офіційно називається «*MAC-48*», походить від специфікації *Ethernet*, оскільки для адреси було передбачено використання 48 бітів. *MAC*-адреси можуть бути «універсально керовані» або «локально керовані».

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант завдання в табл.4.2.
4. Провести порівняльний аналіз вказаних у варіанті технологій *Ethernet* за такими параметрами:
   - специфікація *IEEE*;
   - максимальна швидкість;
   - кабелі;
   - тип (стандарт) кабелів;
   - з'єднувачі;
   - навантаження (термінатори);
   - максимальна довжина сегменту;
   - максимальна кількість з'єднань у сегменті;
   - мінімальна відстань між відгалуженнями;
   - максимальна довжина кабелю;
   - максимальна кількість повторювачів;
   - топологія.
5. Оформити звіт за результатами виконаної роботи.

Таблиця 4.2

Завдання

Номер варіанта	Технології *Ethernet*
1	*10Base5 , 100Base-FX, 1000Base-T, 10GBase-CX4, 40GBase-KR4, 100GBase-KR10*
2	*10Base2, 100Base-T4, 1000Base-TX, 10GBase-SR, 40GBase-CR4, 100GBase-CR10*
3	*StarLAN 10, 100Base-T2, 1000Base-X, 10GBase-LX4, 40GBase-T, 100GBase-SR10*
4	*10Base-T, 100Base-FX, 1000Base-SX, 10GBase-LR, 40GBase-SR4, 100GBase-ER4*
5	*FOIRL, 100Base-TX, 1000Base-LX, 10GBase-SW, 40GBase-LR4, 100GBase-LR4*
6	*10Base-F, 100Base-T4, 1000Base-CX, 10GBase-LW, 40GBase-FR, 100GBase-KR10*
7	*10Base-FB, 100Base-T2, 1000Base-LH, 10GBase-EW, 40GBase-KR4, 100GBase-CR10*
8	*10Base-FL, 100Base-TX, 1000Base-T, 10GBase-T, 40GBase-CR4, 100GBase-LR4*
9	*10Base-FB, 100Base-T4, 1000Base-TX, 10GBase-LW 40GBase-T, 40GBase-SR4*
10	*10Base-FP, 100Base-TX, 1000Base-SX, 10GBase-CX4, 40GBase-LR4, 100GBase-SR10*

Запитання та завдання для самоперевірки

1. Що таке технологія *Ethernet*?
2. Яке позначення *IEEE* має стандарт *Ethernet*?
3. Наведіть структуру кадру *Ethernet* та поясніть зміст кожного його поля.
4. Яке позначення *IEEE* має стандарт *Fast Ethernet*?
5. Вкажіть спільне та відмінне в технологіях *Ethernet* та *Fast Ethernet*.
6. Наведіть загальну характеристику технології *Gigabit Ethernet*.
7. Яке позначення *IEEE* має стандарт *10G Ethernet*?
8. Що таке мережний адаптер?

Лабораторна робота 5
ОЗНАЙОМЛЕННЯ ІЗ СЕРЕДОВИЩЕМ МОДЕЛЮВАННЯ CISCO PACKET TRACER

Мета: ознайомлення з основними мережними пристроями, засобами комунікації з використанням середовища моделювання *Cisco Packet Tracer*.

I. Основні теоретичні відомості

Cisco Packet Tracer – емулятор комп'ютерної мережі, створений компанією *Cisco*. Ця програма дозволяє візуалізувати мережу на логічному та фізичному рівнях, моделювати взаємодію з даними, що передаються мережею.

Загальний вигляд програми показано на рис.5.1.

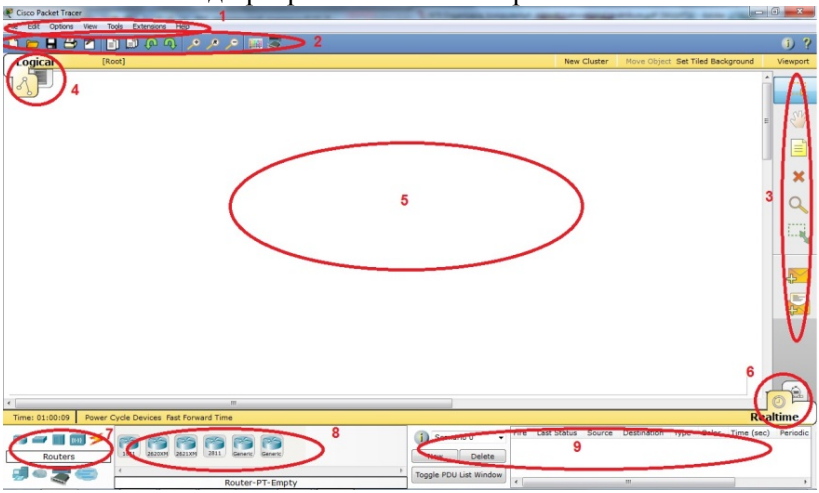

Рис.5.1. Загальний вигляд програми *Cisco Packet Tracer*

Робоча зона вікна програми складається з таких елементів:

1 – ***Menu Bar***, що містить меню *File, Edit, Options, View, Tools, Extensions, Help*.

2 – ***Main Tool Bar***, що містить графічні зображення ярликів для доступу до команд меню *File, Edit, View, Tools* та кнопку *Network Information*.

3 – ***Common Tools Bar***, що забезпечує доступ до часто використовуваних інструментів програми, таких як *Select, Move Layout, Place Note, Delete, Inspect, Add Simple PDU, Add Complex PDU.*

4 – ***Logical/Physical Workspace and Navigation Bar***, що перемикає робочу область з фізичної на логічну і навпаки, а також дозволяє переміщення між рівнями кластера.

5 – ***Workspace***, тобто область для створення мережі, спостереження за симуляцією.

6 – ***Realtime/Simulation Bar***, що дозволяє перемикатися між між режимами Realtime та Simulation Bar.

7 – ***Device Type Selection Box***, що містить доступні типи пристроїв та зв'язків.

8 – ***Device Specific Selection Box***, що використовується для вибору конкретних пристроїв та з'єднань, необхідних для побудови в робочому просторі.

9 – ***User Created Packet Window***, що керує пакетами, які були створені під час симуляції роботи мережі.

Для додавання елементів в робочу область програми необхідно вибрати пристрій на панелі *Network Component*, а потім з панелі *Device Type Selection*. Після цього потрібно натиснути ліву кнопку миші в полі робочої області програми (*Workspace*). Якщо перемістити пристрій прямо з області *Device Type Selection*, то буде вибрана модель пристрою за замовчуванням.

Для кожного елементу користувач може надати ім'я та встановити необхідні параметри. Для цього необхідно натиснути на потрібний елемент лівою кнопкою миші та у вікні, що відкрилося, перейти на вкладку *Config*. Вікно властивостей кожного елементу містить дві вкладки:

- *Physical* – графічний інтерфейс пристрою, що дозволяє симулювати роботу на фізичному рівні;
- *Config* – параметри для налаштування пристрою.

Для видалення непотрібних пристроїв з робочої області використовується кнопка *Delete*.

Для встановлення зв'язків між пристроями використовується панель *Network Component Bar* та вкладка *Connections*. Спочатку необхідно додати в робочу область пристрої, між якими буде встановлено зв'язок, а потім вибрати вкладку *Connections*. Покажчик миші зміниться на курсор у вигляді розніму. Потім необхідно нати-

снути на першому пристрої і вибрати відповідний інтерфейс, далі на другий пристрій, виконавши ту ж операцію. Між пристроями з'явиться кабельне з'єднання, а індикатори на кожному кінці покажуть статус з'єднання (для інтерфейсів, що мають індикатори). Слід зазначити, що кожен тип кабелю може бути сполучений лише з певними типами інтерфейсів. Для автоматичного вибору типу з'єднання слід використовувати *Automatically Choose Connection Type*.

Створена мережа зберігається у файлі з розширенням *.pkt.

Для перемикання між логічним та фізичним представленням мережі слід використовувати *Logical/Physical Workspace* and *Navigation Bar* (відповідає цифрі 4 на рис. 5.1). Область *Logical* використовується для побудови мереж, налаштування, вивчення та усунення несправностей). Область *Physical* містить фізичні розміри логічної топології мережі. Вона дозволяє оцінити масштаб і розташування елементів.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Побудувати комп'ютерну мережу, зображену на рис.5.2.

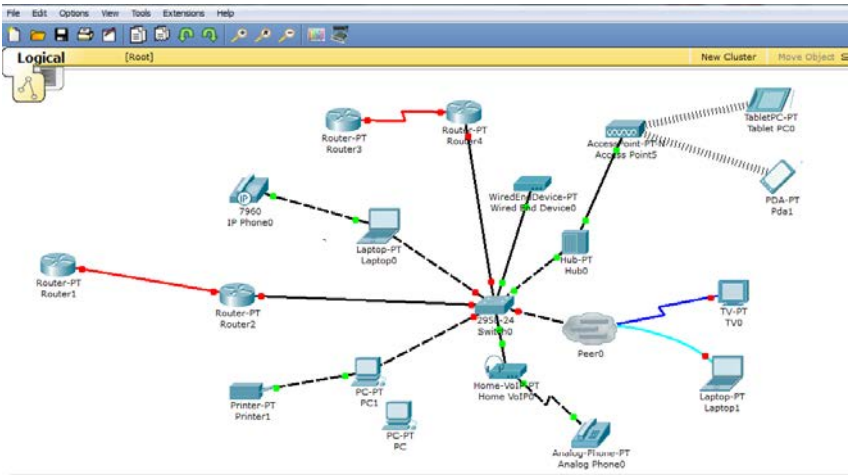

Рис.5.2. Комп'ютерна мережа для дослідження

4. Перейменувати всі пристрої мережі, використавши в назві своє прізвище, наприклад *PC_Ivanov_1*.

5. Визначити всі типи з'єднань між пристроями та заповнити табл. 5.1.

6. Ознайомитися з графічним інтерфейсом кожного пристрою (вкладка *Physical*).

7. Оформити звіт за результатами виконаної роботи.

Таблиця 5.1

Види з'єднань між пристроями

Назва пристрою 1	Назва пристрою 2	Вид з'єднання
Router_Ivanov_1	*Router_Ivanov_2*	оптоволоконний кабель
…..	….	….

Запитання та завдання для самоперевірки

1. З якою метою використовують *Cisco Packet Tracer*?
2. Назвіть основні елементи вікна програми *Cisco Packet Tracer*.
3. Які дії потрібно виконати для додавання елементів в робочу зону?
4. Які види пристроїв доступні для побудови мережі в *Cisco Packet Tracer*?
5. Як називається перемикач між логічною та фізичною областями?
6. З яких елементів складається основне меню програми?
7. Які типи з'єднань реалізовано в *Cisco Packet Tracer*?
8. Які дії потрібно виконати для встановлення з'єднання між пристроями?
9. Як подивитися фізичну комплектацію обладнання, графічний інтерфейс?
10. З яким розширенням зберігаються файли *Cisco Packet Tracer*?
11. Як змінити назву пристрою, що був доданий до мережі?
12. Для чого використовується *Common Tools Bar*?
13. Чи можливий автоматичний вибір типу з'єднання між пристроями?
14. Як додати до робочої зони звичайний текст?
15. Як швидко створити декілька екземплярів одного і того ж пристрою?

Лабораторна робота 6
СИМУЛЯЦІЯ РОБОТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ В CISCO PACKET TRACER. СТРУКТУРА ПАКЕТА

Мета: ознайомлення з режимом симуляції роботи мережі в *Cisco Packet Tracer*, структурою пакета.

Основні теоретичні відомості

Cisco Packet Tracer містить інструмент для симуляції (моделювання) роботи мережі, тобто можна зімітувати будь-які мережні події, проекспериментувати, як буде реагувати мережа в разі збоїв. Наприклад, що станеться, якщо від'єднати будь-який кабель або вимкнути живлення одного з мережних пристроїв.

У режимі моделювання можна не тільки відслідкувати, як пакет передається з одного пристрою на інший, а й подивитися структуру самого пакета. Ознайомимося з даним режимом, побудувавши схему, зображену на рис.6.1.

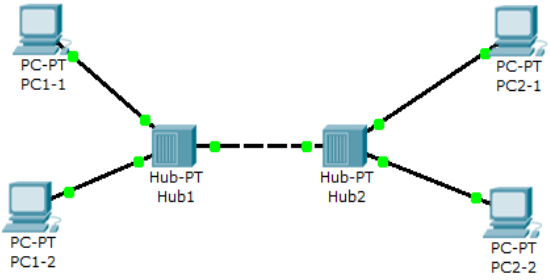

Рис. 6.1. Схема мережі

Після того, як схема мережі побудована, необхідно виконати наступні налаштування: вибрати *PC1-1*, перейти на вкладку *Config*, потім натиснути на *Fast Ethernet* та в полі *IP-Address* ввести 192.168.0.2, натиснути на поле *Subnet Mask* та значення 255.255.255.0 поставиться автоматично. Аналогічні налаштування виконати для *PC1-2, PC2-1, PC2-2*, використавши наступні *IP*-адреси: 192.168.0.3, 192.168.0.4, 192.168.0.5. *IP*-адреси є основним типом адрес, на основі яких мережний рівень передає пакети між мережами.

Для переключення в режим моделювання в правому нижньому кутку виберемо *Simulation*. Відкриється вікно, в якому можна спостерігати за прийнятими та переданими пакетами (рис.6.2).

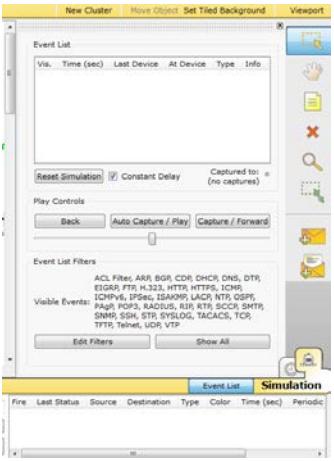

Рис. 6.2. Інтерфейс режиму моделювання

Також для переходу в даний режим можна використати комбінацію клавіш *Shift*+*S*. У вікні, що відкрилося, знаходиться поле подій (*Event List*), кнопка скидання, що очищає список подій (Reset *Simulation*), управління відтворенням (*Back, Auto Capture/Play*, Capture/Forward), а також фільтр протоколів (*Event List Filters*).

Натисніть на кнопку *Edit Filters*, потім зніміть галочку в *Show All*/*None*, поставте галочку поруч із *ICMP* (це мережний протокол, що використовується для передавання повідомлень про помилки та інші виняткові ситуації, що виникають під час передавання даних).

Розглянемо створення пакета, який буде переданий із *PC1-1* на *PC2-2*. Для цього на правій бічній панелі *Common Tools Bar* натисніть на *Add Simple PDU*. Потім натисніть на *PC1-1*, а далі на *PC2-2*. У полі *Event List* видно, що створено пакет. Натиснувши на Auto *Capture*/*Play*, можна спостерігати, як пакет переміщується мережею. Щоб пришвидшити переміщення пакета, перетягніть повзунок вправо (він знаходиться під кнопкою *Auto Capture*/*Play*). Якщо необхідно вручну переміщати пакет, необхідно натиснути на *Capture*/ *Back* або *Forward.*

У режимі Realtime можна виконати аналогічні дії зі створення пакета, результат передавання можна подивитися на панелі ***User***

Created Packet Window у вигляді повідомлення *Successful* або *Failed*.

Якщо в режимі моделювання у вікні *Event List* натиснути на кольоровий значок пакета в колонці *Info*, то відкриється вікно, в якому можна переглянути структуру відправленого та прийнятого пакета на різних етапах пересилання повідомлення та відповідні рівні моделі *OSI*, які він проходить (рис. 6.3, рис. 6.4).

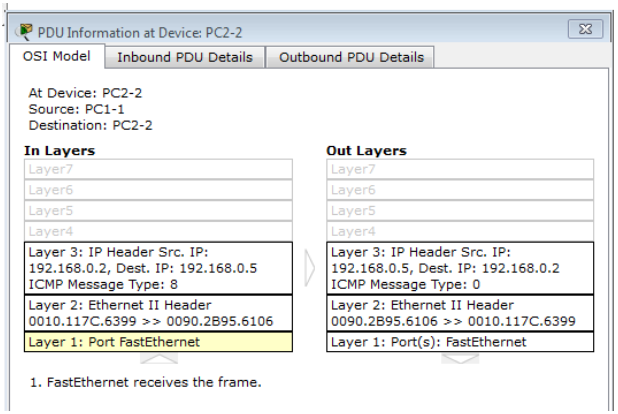

Рис. 6.3. Моніторинг роботи на моделі *OSI*

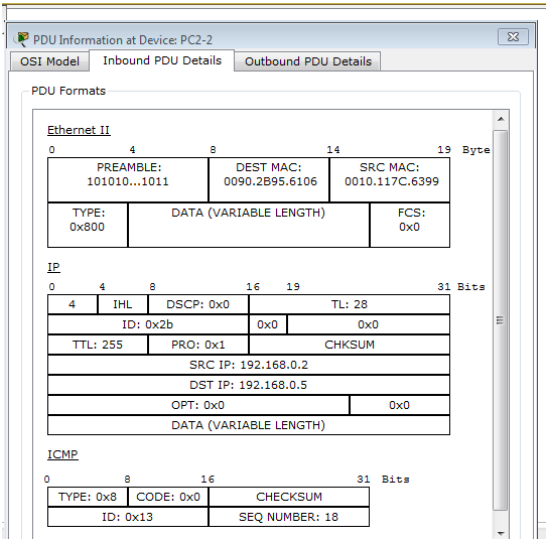

Рис.6.4. Структура пакета

На рис. 6.4 видно, як формується пакет, з яких полів складається та якими даними наповнюється. Так, пакет *Ethernet II* складається з наступних полів:

- преамбула *PREAMBLE* (7 байтів, 101010…1011), використовується для синхронізації;
- *DEST MAC* (6 байтів), адреса отримувача (адреса мережного адаптера в 16-й системі числення);
- *SRC MAC* (6 байтів), адреса відправника (адреса мережного адаптера в 16-й системі числення);
- *TYPE* (2 байти) – тип для позначення типу протоколу, використовується для позначення відмінності між *DIX Ethernet* та *IEEE 802.3*;
- *DATA* (змінна довжина байтів) – дані, що пересилаються;
- *FCS* (*Frame Check Sequence*) 4 байти, поле контрольної суми. Пристрій-передавач обчислює контрольну суму та записує її в це поле. Приймаючий пристрій виконує аналогічний розрахунок і порівнює з величиною, записаною в полі, щоб впевнитися, що пакет передано без помилок.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Побудувати комп'ютерну мережу, зображену на рис.6.5.

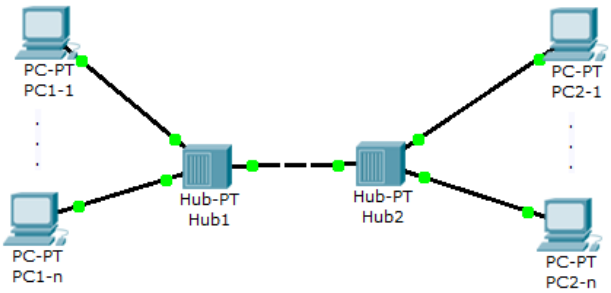

Рис. 6.5. Комп'ютерна мережа для дослідження

Вибрати кількість пристроїв та дані для їх налаштування відповідно до варіанта в табл.6.1.

Таблиця 6.1

Кількість пристроїв та дані для їх налаштування

Номер варіанта	Кількість *PC*, що під'єднані до *Hub-1* та їх *IP*-адреси	Кількість *PC*, що під'єднані до *Hub-2* та їх *IP*-адреси
1	3; 192.168.0.31-192.168.0.33	5; 192.168.0.51-192.168.0.55
2	4; 192.168.0.41-192.168.0.44	6; 192.168.0.61-192.168.0.66
3	5; 192.168.0.51-192.168.0.55	6; 192.168.0.61-192.168.0.66
4	6; 192.168.0.61-192.168.0.66	5; 192.168.0.51-192.168.0.55
5	3; 192.168.0.31-192.168.0.33	4; 192.168.0.41-192.168.0.44
6	4; 192.168.0.41-192.168.0.44	3; 192.168.0.31-192.168.0.33
7	5; 192.168.0.51-192.168.0.55	4; 192.168.0.41-192.168.0.44
8	6; 192.168.0.61-192.168.0.66	3; 192.168.0.31-192.168.0.33
9	3; 192.168.0.31-192.168.0.33	5; 192.168.0.51-192.168.0.55
10	4; 192.168.0.41-192.168.0.44	6; 192.168.0.61-192.168.0.66

4. Створити прості пакети, які будуть передані від *PC1-1* до *PC2-n* та від *PC2-1* до *PC1-n*, де *n* – кількість пристроїв, відповідно до варіанта.

5. У режимі моделювання відслідкувати проходження пакетів. Зробити скріншоти та записати пояснення у звіт.

6. Ознайомитися етапами проходження пакетів відповідно до рівнів моделі OSI та записати пояснення у звіт.

7. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Як відкрити режим симуляції в *Cisco Packet Tracer*?
2. З якою метою використовується режим моделювання в *Cisco Packet Tracer*?
3. Назвіть основні елементи вікна моделювання. Для чого вони використовуються?
4. Як створити пакет для передавання між пристроями?
5. Які кнопки керування переміщення пакета ви знаєте?
6. Як відкрити вікно для перегляду структури відправленого та прийнятого пакета на різних етапах пересилання повідомлення та відповідні рівні моделі *OSI*, які він проходить?
7. Назвіть структуру пакета *Ethernet II*.
8. Назвіть основні відмінності в структурі пакетів залежно від стандарту *Ethernet*.

Лабораторна робота 7
MAC-АДРЕСИ ТА ЇХ ЗАСТОСУВАННЯ У СУЧАСНИХ МЕРЕЖАХ

Мета: вивчення загальних принципів адресації у сучасних комп'ютерних мережах, ознайомитися зі структурою, видами та застосуванням *MAC*-адрес, отримати практичні навички аналізу та визначення параметрів *MAC*-адрес.

Основні теоретичні відомості

Для того, що б в мережі *Ethernet* стала можливою доставка пакетів, необхідна певна система адресації. Кожен вузол має унікальний спосіб ідентифікації – фізичну адресу, яку в *Ethernet* називають *MAC*-адресою (*Media Access Control*, адреса керування доступом до середовища передавання). Вона записана в мережному адаптері ПК або мережних інтерфейсах пристроїв. *MAC*-адреса має довжину 48 бітів і записується у вигляді шістнадцяткових цифр, наприклад *0C-8B-FD-93-63-EB* (формат запису *IEEE EUI-48*). Можливий й інший формат запису *MAC*-адреси 0c:8b:fd:93:63:eb (формат запису Unix Zero-Padded) або 0c8b.fd93.63eb (формат запису Cisco). У деяких випадках запис MAC-адреси здійснюється без роздільників, як проста послідовність із шести байтів.

Керування загальним адресним простором MAC-адрес здійснює Інститут інженерів з електротехніки та електроніки (*IEEE, Institute of Electrical and Electronics Engineers*). Увесь адресний простір розбивається на три підпростори, які позначаються як *MAC-48, EUI-48, EUI-64*. Відмітності між *MAC-48* і *EUI-48* є номінальними: *MAC-48* застосовується для ідентифікації мережних адаптерів/інтерфейсів, *EUI-48* – для ідентифікації інших пристроїв та програм. *EUI-64* є розширенням *EUI-48*.

MAC-адреса складається з двох однакових за довжиною 24-бітних блоків:

- *OUI (Organizationally Unique Identifier)* – унікальний ідентифікатор виробника;
- *OUA (Organizationally Unique Address)* – унікальний ідентифікатор адаптера/інтерфейса.

Блок *OUI* містить у старшому байті два біти *I/G* (*Individual/Group Bit*) та *G/L* (*Global/Local Bit*). *I/G* – ознака уніка-

льної чи групової широкомовної адреси, *G/L* – ознака глобальної чи локальної адреси.

Адресний простір *MAC*-48 контролюється *IEEE* таким чином, щоб забезпечити дотримання унікальності *MAC*-адрес. Будь-який виробник мережних адаптерів/інтерфейсів подає заявку на отримання одного або діапазону унікальних *OUI*. Після отримання *OUI* на виробника покладається функція контролю унікальності *OUA*. Слід зазначити, що деякі *OUI* застосовуються для спеціальних цілей. Детальну інформацію про зареєстровані за виробниками *OUI* та *OUA* можна отримати на вебсайті *IEEE* за адресами:

- http://standards-oui.ieee.org/oui/oui.txt
- http://standards-oui.ieee.org/cid/cid.txt.

Наведемо приклад визначення, якою (унікальною, груповою, широкомовною) та у яких випадках (адреса відправника, адреса отримувача) може застосовуватися *MAC*-адреса *00-27-10-DB-79-B3*, а також визначити виробника мережного адаптера.

Спочатку необхідно записати старший байт *MAC*-адреси у двійковій системі числення: *0C*=00000000. Молодші два біти дають змогу визначити, якою є *MAC*-адреса. Оскільки молодший біт *G/L*=0 та наступний за ним біт *I/G*=0, то можна зробити висновок, що дана *MAC*-адреса є унікальною глобальною адресою, тобто може бути призначена мережному адаптеру/інтерфейса і може застосовуватися як адреса відправника, і як адреса отримувача.

Для визначення виробника, якому виділений *OUI* (00-27-10), можна скористатися пошуковою системою https://www.macvendorlookup.com/, результати пошуку наведені на рис.7.1.

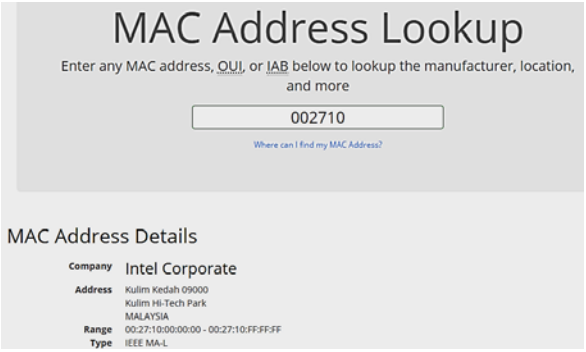

Рис.7.1. Результат пошуку *OUI* виробника

Ідентифікатор виробника виділено для *Intel Corporate*, діапазон можливих адрес - *00:27:10:00:00:00-00:27:10:FF:FF:FF*.

Розглянемо, як отримати *MAC*-адресу пристрою в емуляторі *Cisco Packet Tracer*. Якщо необхідно отримати *MAC*-адресу хоста (*PC*), то її можна подивитися у вкладці *Config*. Мережний комутатор (switch) призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента та передає дані лише безпосередньо отримувачу. Комутатор працює на канальному рівні моделі *OSI*, і тому в загальному випадку може тільки поєднувати вузли однієї мережі за їхніми *MAC*-адресами.

Комутатор зберігає в пам'яті таблицю, у якій вказуються відповідні *MAC*-адреси вузла порту комутатора. Під час увімкнення комутатора ця таблиця порожня, і він працює в режимі навчання. У цьому режимі дані, що поступають на який-небудь порт передаються на всі інші порти комутатора. Комутатор аналізує кадри й, визначивши *MAC*-адресу хоста-відправника, заносить його до таблиці. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, *MAC*-адреса якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо *MAC*-адреса хоста-отримувача ще не відома, то кадр буде продубльований на всі інтерфейси. Згодом комутатор будує повну таблицю для всіх своїх портів, і в результаті трафік локалізується.

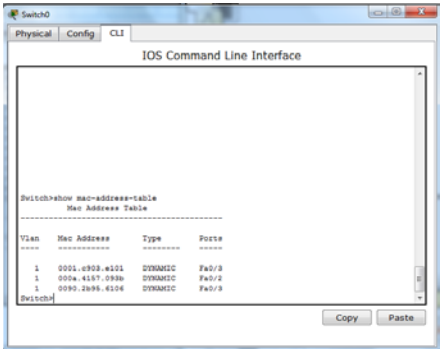

Рис. 7.2. Таблиця *MAC*-адрес комутатора

Щоб подивитися таблицю *MAC*-адрес комутатора, необхідно перейти в його налаштуваннях на вкладку *CLI* (*Command Line*

Interface), ввести в командному рядку *show* mac-*address-table* (рис.7.2).

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитись з довідковою літературою.
3. Побудувати комп'ютерну мережу, наведену на рис.7.3. Вибрати кількість пристроїв та дані для їх налаштування відповідно до варіанта в табл.7.1.

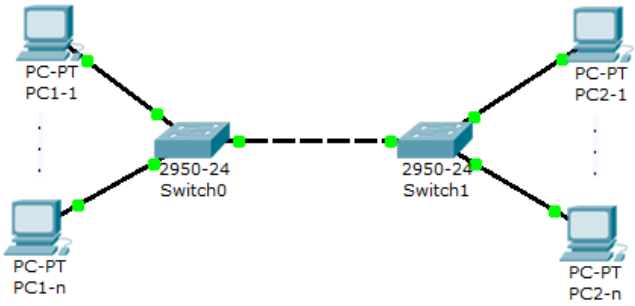

Рис.7.3. Комп'ютерна мережа для дослідження

Таблиця 7.1

Кількість пристроїв та дані для їх налаштування

Номер варіанта	Кількість *PC*, що під'єднані до *Switch-0* та їх *IP*-адреси	Кількість *PC*, що під'єднані до *Switch* -1 та їх *IP*-адреси
1	4; 192.168.0.41-192.168.0.44	6; 192.168.0.61-192.168.0.66
2	3; 192.168.0.31-192.168.0.33	5; 192.168.0.51-192.168.0.55
3	4; 192.168.0.41-192.168.0.44	6; 192.168.0.61-192.168.0.66
4	5; 192.168.0.51-192.168.0.55	6; 192.168.0.61-192.168.0.66
5	6; 192.168.0.61-192.168.0.66	5; 192.168.0.51-192.168.0.55
6	3; 192.168.0.31-192.168.0.33	4; 192.168.0.41-192.168.0.44
7	4; 192.168.0.41-192.168.0.44	3; 192.168.0.31-192.168.0.33
8	5; 192.168.0.51-192.168.0.55	4; 192.168.0.41-192.168.0.44
9	6; 192.168.0.61-192.168.0.66	3; 192.168.0.31-192.168.0.33
10	3; 192.168.0.31-192.168.0.33	5; 192.168.0.51-192.168.0.55

4. Записати *MAC*-адреси всіх пристроїв побудованої мережі.

5. Дослідити таблиці *MAC*-адрес для *Switch-0* та *Switch-1*. Порівняти отримані результати.

6. Визначити формат запису; якими (унікальними, груповими, широкомовними) є задані *MAC*-адреси (табл.7.2); у яких випадках (як адреси відправників чи як адреси отримувачів) можуть застосовуватися ці *MAC*-адреси; записати їх *OUI* та *OUA* частини.

Таблиця 7.2

MAC-адреси для дослідження

Номер варіанта	*MAC*-адреси		
1	*8D:42:18:B0:6C:E4*	*97-36-FD-25-40-08*	*9A2E.A42F.1A1C*
2	*89:D9:65:16:E3:FE*	*86-12-8D-C0-9D-90*	*EA50.E420.B519*
3	*85:1C:8B:50:89:2A*	*0B-35-75-40-D7-7C*	*2081.BF14.9323*
4	*2D:A8:99:D1:2A:A8*	*59-19-A1-12-82-40*	*7528.F34D.E9DC*
5	*FB:EE:EE:C7:3D:3C*	*01-09-EA-9E-5D-3C*	*EFC9.5D27.EA89*
6	*88:C1:2F:B4:C5:C6*	*27-DF-E4-B3-DD-C7*	*99D2.CF63.48C3*
7	*E9:70:32:93:D7:1C*	*EE-A6-0E-70-F7-9D*	*C00A.AD68.D212*
8	*5D:39:A6:52:E1:30*	*13-B7-0E-32-50-24*	*F39D.D167.B397*
9	*0E:4D:41:32:AA:3E*	*4D-72-A4-99-23-F2*	*3FB7.87B4.7BE1*
10	*CC:1A:32:69:F9:29*	*26-31-EC-FF-FA-6F*	*9496.6A85.D13B*

7. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Що таке *MAC*-адреса?
2. Наведіть приклади *MAC*-адрес.
3. Які існують формати запису *MAC*-адреси?
4. Яка структура *MAC*-адреси?
5. Що таке унікальний ідентифікатор виробника?
6. Що таке унікальний ідентифікатор адаптера?
7. Де можна подивитися детальну інформацію про зареєстровані за виробниками *OUI* та *OUA*?
8. Яке призначення бітів *G/L* та *I/G*?
9. Як отримати *MAC*-адресу хоста в *Cisco Packet Tracer*?
10. Яке призначення комутатора?
11. Як заповнюється таблиця *MAC*-адрес комутатора?
12. Як подивитися таблицю *MAC*-адрес комутатора?

Лабораторна робота 8
ЗНАЙОМСТВО З КОМАНДАМИ ОПЕРАЦІЙНОЇ СИСТЕМИ CISCO

Мета: вивчення режимів функціонування *Cisco IOS*, інтерфейсу користувача та основними командами конфігурування комутаторів.

Основні теоретичні відомості

Мережне обладнання компанії *Cisco* працює на базі операційної системи *Cisco IOS* (*Internetworking Operating System*). Ця операційна система забезпечує роботу основних служб комутації та маршрутизації, надійний та безпечний доступ до мережних ресурсів, надання засобів масштабування мережі.

У *Cisco IOS* є три режими роботи: *ROM*-монітор, завантаження з ROM, повнофункціональний режим *Cisco IOS*. Перший режим працює здебільшого при несправностях у маршрутизаторах або у випадку відновлення пароля. Запрошення у цьому режимі має вигляд > або *ROMMON*>.

Режим завантаження з ROM використовується для заміни образу операційної системи. Програмне забезпечення *ROM*-монітора виконує процес початкового завантаження і забезпечує роботу та діагностику апаратного забезпечення на нижньому рівні. Доступ до цього режиму можливий тільки через консольний сеанс. Запрошення у цьому режимі має вигляд *Router (boot)*>.

Повнофункціональний режим *Cisco IOS*. У процесі запуску в нормальному режимі комутатор завантажує *IOS* в *RAM*. Для визначення або встановлення параметрів завантаження використовується конфігураційний регістр. Запрошення в цьому режимі має вигляд *Router*> або *Switch*>.

Як традиційне інтерактивне середовище в *Cisco IOS* використовується інтерфейс командного рядка *CLI* (Command Line *Interface*). *CLI* має ієрархічну структуру, тобто для виконання різних завдань необхідний перехід в різні режими. В кожному з них командний рядок має різні мітки запрошення, що дозволяє адміністратору не плутати режими і використовувати тільки ті команди, що підтримуються даним режимом.

Використовується два рівні доступу – користувацький (*User Executive Mode*) та привілейований (*Privileged Executive Mode*). В користувацькому режимі доступний лише обмежений набір основ-

них команд, які дозволяють проводити моніторинг та не допускаються зміни файла конфігурації. Часто його називають режимом перегляду. У командному рядку цей режим ідентифікується символом >.

Привілейований режим доступу дає можливість використовувати всі команди операційної системи. Доступ до нього авторизований та може бути обмежений логіном та паролем. У командному рядку цей режим ідентифікується символом #.

Для переходу з користувацького у привілейований режим необхідно ввести команду *enable*, а для зворотного переходу – *disable*.

З привілейованого режиму можна отримати доступ до режиму глобального конфігурування *(config)#*. В ньому налаштовують глобальні параметри та є можливість переходу в специфічний режим конфігурування *(config-mode)#*, де mode означає який саме режим, наприклад, конфігурування інтерфейсу *(config-if)#*, підінтерфейсу *(config-subif)#*, лінії *(config-line)#*, маршрутизації *(config-router)#*.

Для отримання довідки щодо тієї чи іншої команди необхідно набрати знак питання ?, також можна уточнити будь-яку команду та її формат. Якщо знак питання ставиться безпосередньо у слові команди, то виводиться список команд, що починаються на відповідні початкові літери, якщо після команди – то виводиться формат відповідного аргументу.

Під час роботи в *CLI* можна отримати наступні види повідомлення про помилки:

- *Ambiguous command* – введена команда (її частина) є неоднозначною і не дозволяє визначити, яку саме команду було введено.
- *Incomplete command* – команду введено неповністю, не введені всі її аргументи.
- *Incorrect command* – команду введено некоректно (неправильно введено команду або її аргументи, місце помилки позначається символом ^).

Розглянемо деякі приклади команд початкового конфігурування та моніторингу комутатора.

Настроювання банера. Банером називається повідомлення, що відображається під час входу до системи (*Message Of The Day, MOTD*):

Switch(config)#banner motd #

Enter TEXT message. End with the character '#'.

Laboratory assignment #

Ім'я хосту. Це ім'я відображається перед символом > або #:

Switch(config)#hostname MySwitch

Результатом виконання цієї команди буде: *MySwitch#*

Пароль доступу. Дозволяє контролювати доступ до комутатора в привілейованому режимі. Встановимо пароль «*compnet*»:

MySwitch(config)#enable password compnet

Щоб перевірити, чи пароль встановлено, поверніться до режиму перегляду і спробуйте зайти в привілейований режим. Результат:

MySwitch>en

Password:

Зверніть увагу, що символи, які вводяться як пароль, користувачу не видно. Якщо пароль введено невірно, система знову попросить його ввести.

Файли конфігурації комутатора містять команди його налаштування та служб. Є два файли конфігурації: робочий (*Running Config*), що зберігається в *RAM* та втрачається після перезавантаження, оскільки пам'ять *RAM* залежна від живлення; стартовий (*Startup Config*), що незалежний від живлення, зберігається в NVRAM і копіюється в *RAM* під час запуску системи. Після будь-яких внесень змін у конфігурацію комутатора, ці зміни можна перевірити за допомогою команди *show running-config*, що відображає поточну конфігурацію. Для збереження конфігураційних змін в *NVRAM* слід ввести команду, та вказати потім файл збереження:

MySwitch#copy running-config startup-config

Destination filename [startup-config]? startup-config

Building configuration...

[OK]

В операційній системі ряд команд *show* надають статичну інформацію стосовно роботи пристрою. Наприклад, вони дозволяють отримати інформацію щодо конфігурації, функціонування та статусу частин комутатора. Так, наприклад, команда *show mac-address-table* відображає таблицю *MAC*-адрес комутатора. Команда *clear mac-address-table* вилучає позиції таблиці з адресами, що стали недійсними.

Слід зазначити, що ряд команд *IOS* є спільними як для комутатора, так і для маршрутизатора.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Додати до робочої області один комутатор. Перейти в інтерфейс командного рядка.
4. Додати банер, вказавши в ньому своє прізвище, назву дисципліни, дату виконання роботи.
5. Змінити назву комутатора, вказавши в назві своє прізвище.
6. Задати пароль на вхід в привілейований режим.
7. Перевірити роботу, записати призначення та результати виконання наступних команд:

show version, show interfaces, show users, show running-config, show start-up-config, copy running-config startup-config, enable secret password, show mac-address-table, clear mac-address-table.

8. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Поясніть роль, призначення та функції *Cisco IOS*.
2. Поясніть, яким чином можна отримати доступ до конфігурування мережного обладнання *Cisco IOS*.
3. Наведіть та стисло охарактеризуйте режими роботи *Cisco IOS*.
4. Наведіть призначення та типи файлів конфігурації комутатора.
5. Поясніть важливість налаштування імені комутатора та наведіть відповідні команди.
6. Поясніть, що можна захистити паролями під час роботи з комутатором. Наведіть відповідні команди.
7. Яке призначення банерів? Наведіть команди їх налаштування.
8. Які команди застосовуються для перегляду та очищення таблиці *MAC*-адрес комутатора?
9. Поясніть, з якою метою використовуються команди групи *Show*. Наведіть кілька таких команд та поясніть їх призначення.
10. Яку інформацію можна отримати в результаті виконання команди *show version*?

Лабораторна робота 9
ВІРТУАЛЬНІ ЛОКАЛЬНІ МЕРЕЖІ

Мета: ознайомлення з віртуальними локальними мережами, створення та налаштування в *Cisco Packet Tracer VLAN* на комутаторі.

Основні теоретичні відомості

Віртуальна локальна мережа (*Virtual Local Area Network, VLAN*) – це комутований сегмент мережі, який логічно виділений відповідно до виконуваних функцій, груп або застосування, незалежно від фізичного розташування користувачів. Віртуальні локальні мережі мають всі властивості фізичних локальних мереж, але робочі станції можна групувати, навіть якщо фони фізично розташовані не в одному сегменті. Це можливо завдяки тому, що будь-який порт комутатора можна налаштувати на приналежність до певної *VLAN*. У такому випадку одноадресний, багатоадресний і широкомовний трафік буде передаватися тільки між робочими станціями, що належать одній *VLAN*.

Кожна *VLAN* розглядається як логічна мережа, тобто пакети, призначені станціям, які не належать даній *VLAN*, повинні передаватися через маршрутизуючий пристрій (маршрутизатор або комутатор 3-го рівня). Таким чином, за допомогою віртуальних локальних мереж вирішується проблема обмеження області передавання широкомовних пакетів і викликаних ними наслідків, які суттєво знижують продуктивність мережі, викликають широкомовні шторми.

Типи *VLAN*:

- *VLAN* на основі портів (*Port-based* VLAN) – кожний порт комутатора призначається в певну *VLAN* і будь-який мережний пристрій, підключений в даний порт, буде знаходитись в призначеній віртуальній мережі;
- *VLAN* на основі *MAC*-адрес (*MAC-based VLAN*) – членство в *VLAN* ґрунтується на *MAC*-адресі робочої станції. У цьому випадку на комутаторі необхідно створити прив'язку *MAC*-адрес усіх пристроїв до *VLAN*;
- *VLAN* на основі портів і протоколів *IEEE 802.1v* – тип протоколу й порт використовуються для визначення членства в *VLAN*;

- *VLAN* на основі стандарту *IEEE 802.1Q* – поле приналежності *VLAN*, інтегрується в структуру кадра *Ethernet*, що дозволяє передавати дану інформацію мережею. Перевагою є гнучкість налаштування, використання не тільки на одному комутаторі, але й у межах усієї мережі, що комутується; можливість використання обладнання різних виробників для організації мережі. Даний тип *VLAN* використовується частіше інших.

Існують два методи призначення порту в певну *VLAN*: статичне призначення (приналежність порту *VLAN* задається адміністратором у процесі налаштувань) та динамічне призначення (приналежність порту *VLAN* визначається у ході роботи комутатора за допомогою процедур, описаних у спеціальних стандартах, таких, як *IEEE 802.1X*.

Розглянемо налаштування *VLAN* в *Cisco Packet Tracer*. Побудуємо схему мережі, що складається з одного комутатора *Cisco 2964TT* та 5 *PC* (рис.9.1).

Будемо вважати, що *PC1*, *PC2*, *PC3* знаходяться в *VLAN2*, *PC4*, *PC5* – в *VLAN* 3.

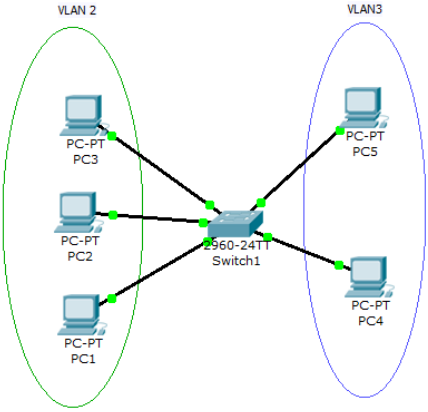

Рис. 9.1. Схема мережі з одним комутатором

У табл. 9.1 наведені адреси комп'ютерів.

У режимі реального часу перевіримо зв'язність отриманої мережі – надішлемо пакети від *PC1* до *PC3* та від *PC4* до *PC5*. Результат виконання обох операцій має бути Successful. Якщо надіслати пакети від *PC3* до *PC5* – то вони не дійдуть, оскільки

комп'ютери знаходяться в різних підмережах (отримаємо статус Failed).

Таблиця 9.1

PC	*IP*-адреса	Порт комутатора
PC1	10.0.0.1	1
PC2	10.0.0.2	2
PC3	10.0.0.3	3
PC4	192.168.0.1	4
PC5	192.168.0.2	5

Перейдемо до налаштувань комутатора. Відкриємо вікно консолі *CLI*. Перейдемо в привілейований режим та переглянемо інформацію про існуючі на комутаторі *VLAN*, використавши команду *sh vl br* (рис.9.2).

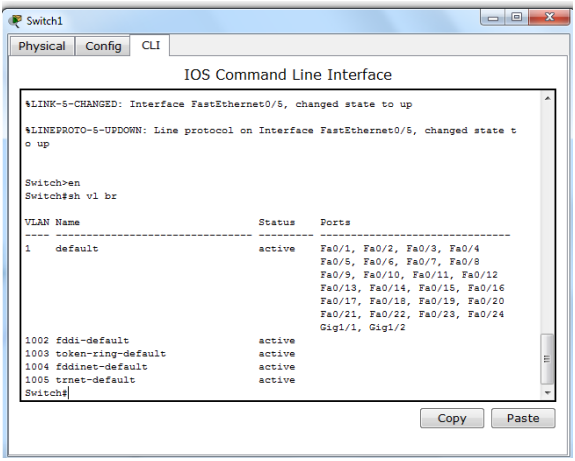

Рис.9.2. Перегляд інформації про *VLAN* на комутаторі

Перший стовпчик – це *номер VLAN*, другий стовпчик – назва *VLAN*, третій – стан *VLAN* (працює він в даний момент чи ні), четвертий стовпчик – приналежність портів до *VLAN*. Як бачимо, за замовчуванням в комутаторі працює п'ять *VLAN* і всі порти комутатора за замовчуванням належать до *VLAN1*. Решта чотири *VLAN* є службовими і використовуються не дуже часто.

Для реалізації мережі на рис.9.1 необхідно створити ще два *VLAN*. Виконаємо для цього наступну команду:

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#VLAN 2
Switch(config-vlan)#name subnet_10
Switch(config-vlan)#interface range fastEthernet 0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#

Даними командами ми створили на комутаторі *VLAN2* з ім'ям *subnet_10*, сконфігурували інтерфейси *fastEthernet 0/1-3*. Команда *switchport mode access* конфігурує обраний порт комутатора як порт доступу. Вийдемо з режиму конфігурації і переглянемо результат конфігурації (рис.9.3).

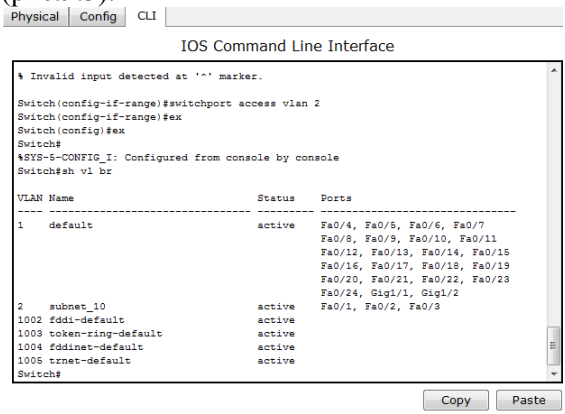

Рис. 9.3. Розподіл портів *VLAN*

Як бачимо, на комутаторі з'явився ще один *VLAN* з номером 2 та ім'ям subnet_10.

Аналогічним чином створимо *VLAN3* з ім'ям subnet_192 і зробимо його портами доступу інтерфейси *fastEthernet* 0/4-5:

Switch(config)#VLAN 3
Switch(config-vlan)#name subnet_192
Switch(config-vlan)#interface range fastEthernet 0/4-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 3

Мережа налаштована і залишилося її протестувати. Надішлемо пакети від *PC1* до *PC3* та від *PC1* до *PC5* – результати попередніх тестувань не змінилися. Тепер задамо *PC4* адресу 10.0.0.13, а *PC5* адресу 10.0.0.14 і знову в режимі реального часу повторимо надсилання пакетів. Як бачимо, знову нічого не змінилося, хоча всі п'ять комп'ютерів теоретично знаходяться в одній підмережі і повинні бачити один одного. На практиці відповідно до зроблених налаштувань *PC1*, *PC2*, *PC3* та *PC4*, *PC5* знаходяться в різних віртуальних мережах і тому не можуть взаємодіяти між собою.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Побудувати комп'ютерну мережу, що буде складатися з восьми *PC*, що під'єднані до одного комутатора. Налаштування провести відповідно до варіанта в табл. 9.2.

Таблиця 9.2

Варіанти завдань

Номер варіанта	*VLAN1*				*VLAN2*			
	PC1	*PC2*	*PC3*	*PC4*	*PC5*	*PC6*	*PC7*	*PC8*
1	10.0.0.10	10.0.0.11	10.0.0.12	10.0.0.13	192.168.0.1	192.168.0.2	192.168.0.3	192.168.0.4
2	10.0.0.20	10.0.0.21	10.0.0.22	10.0.0.23	192.168.0.2	192.168.0.3	192.168.0.4	192.168.0.5
3	10.0.0.30	10.0.0.31	10.0.0.32	10.0.0.33	192.168.0.3	192.168.0.4	192.168.0.5	192.168.0.6
4	10.0.0.40	10.0.0.41	10.0.0.42	10.0.0.43	192.168.0.4	192.168.0.5	192.168.0.6	192.168.0.7
5	10.0.0.50	10.0.0.51	10.0.0.52	10.0.0.53	192.168.0.5	192.168.0.6	192.168.0.7	192.168.0.8
6	10.0.0.60	10.0.0.61	10.0.0.62	10.0.0.63	192.168.0.6	192.168.0.7	192.168.0.8	192.168.0.9
7	10.0.0.70	10.0.0.71	10.0.0.72	10.0.0.73	192.168.0.7	192.168.0.8	192.168.0.9	192.168.0.10
8	10.0.0.80	10.0.0.81	10.0.0.82	10.0.0.83	192.168.0.8	192.168.0.9	192.168.0.10	192.168.0.11
9	10.0.0.90	10.0.0.91	10.0.0.92	10.0.0.93	192.168.0.9	192.168.0.10	192.168.0.11	192.168.0.12
10	10.0.0.10	10.0.0.11	10.0.0.12	10.0.0.13	192.168.0.10	192.168.0.11	192.168.0.12	192.168.0.13

4. Виконати налаштування двох віртуальних локальних мереж. Перевірити зроблені налаштування, замінивши *IP*-адреси *VLAN2* на довільні адреси з мережі 10.0.0.0/8.
5. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Яке призначення *VLAN*?
2. Які вимоги до створення *VLAN*?
3. Як перевірити, чи були створені віртуальні локальні мережі на комутаторі?
4. Які переваги віртуальних локальних мереж?
5. Які типи *VLAN* ви знаєте?
6. Які методи призначення порту в *VLAN* ви знаєте?
7. Назвіть команди конфігурування *VLAN*.

Лабораторна робота 10
НАЛАШТУВАННЯ VLAN НА ДВОХ КОМУТАТОРАХ CISCO

Мета: навчитися створювати *VLAN* на двох комутаторах в *Cisco Packet Tracer*.

Основні теоретичні відомості

Досить часто на практиці виникає завдання поділу пристроїв, підключених до одного або декількох комутаторів, на кілька віртуальних мереж. В такому випадку між комутаторами крім даних необхідно передавати інформацію, до якої локальної мережі відноситься кадр. Для цього був розроблений стандарт *802.1Q*. Комутатори між собою з'єднуються через транковий (*trunk*) канал.

Розглянемо налаштування віртуальних мереж на двох комутаторах. Побудуємо мережу, схема якої показана на рис.10.1.

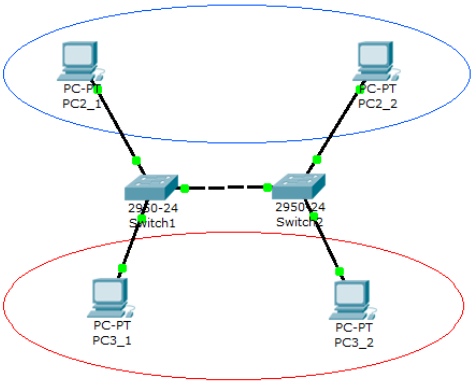

Рис. 10.1. Схема мережі

У табл. 10.1 наведені адреси комп'ютерів.

Таблиця 10.1

PC	*IP*-дреса	Комутатор	Порт комутатора	*VLAN*
PC2_1	10.0.0.1	*Switch1*	1	*VLAN20*
PC2_2	10.0.0.3	*Switch2*	1	*VLAN20*
PC3_1	10.0.0.2	*Switch1*	2	*VLAN30*
PC3_2	10.0.0.4	*Switch2*	2	*VLAN30*

Перевіримо, чи надходять пакети всередині мережі. Для цього в режимі реального часу надішлемо пакети від *PC2_1* до *PC2_2*, *PC2_1*, *PC3_2*. Якщо мережа налаштована правильно, результатом виконання буде повідомлення Successful.

Тепер налаштуємо віртуальні мережі *VLAN20* та *VLAN30*. Відкриємо *CLI* для *Switch1* та введемо наступні команди:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
Switch(config)#vlan 30
Switch(config-vlan)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
```

Перегляньте конфігурацію про *VLAN*, які налаштовані на *Switch1* за допомогою команди *sh vl br* (рис.10.2).

Аналогічні налаштування зробимо для *Switch2*. Якщо зараз спробувати надіслати пакети на будь-який PC, то вони не будуть доставлені, оскільки нема налаштування між комутаторами. Тепер організуємо магістраль обміну між комутаторами. Для цього налаштуємо третій порт на кожному комутаторі як транковий. Для *Switch1*:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet 0/3
```

Switch(config-if)#switchport mode trunk

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if)#no shutdown

Switch(config-if)#ex

Switch(config)#

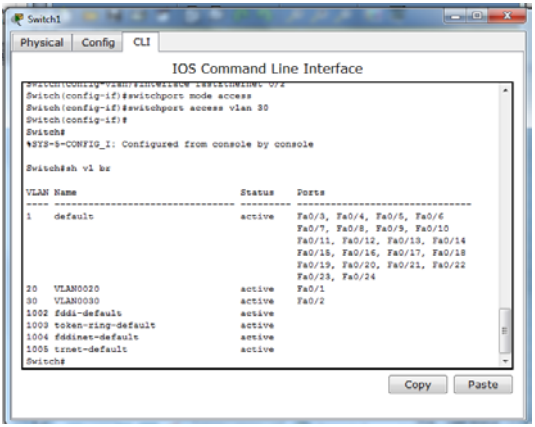

Рис. 10.2 Конфігурація *Switch1*

Відкрийте конфігурацію комутатора на інтерфейсі *FastEthernet* 0/3 та переконайтеся, що порт транковий (рис.10.3).

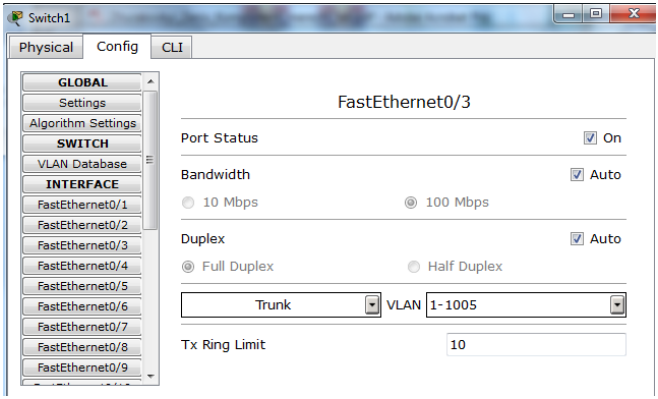

Рис. 10.3. Конфігурація інтерфейсу *FastEthernet 0/3*

На комутаторі *Switch2* інтерфейс *FastEthernet 0/3* автоматично налаштується як транковий. Тепер спробуємо надіслати пакет з *PC2_1* на *PC2_2*. Тепер пакет буде доставлено. Аналогічно буде доставлено пакет з *PC3_1* на *PC3_2*. Пакети з *PC2_1* на *PC3_1* не будуть доставлені, оскільки комп'ютери знаходяться в різних *VLAN*.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Побудувати комп'ютерну мереж, що буде складатися з трьох комутаторів (рис.10.4).

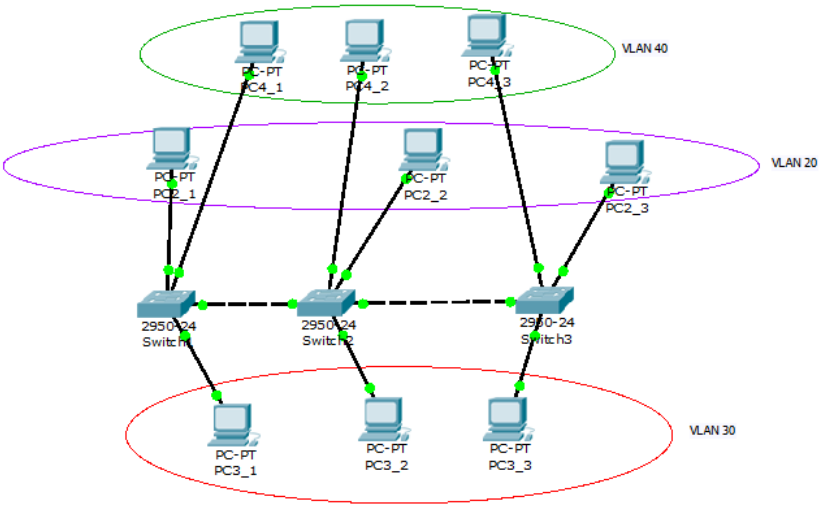

Рис. 10.4. Схема мережі

Налаштування провести відповідно до варіанта в табл. 10.2.

4. Налаштувати транк-порти між комутаторами *Switch1*, *Switch2*, *Switch3*.
5. Перевірити з'єднання всередині кожної *VLAN* та між ними.
6. Оформити звіт за результатами виконаної роботи.

Таблиця 10.2

Варіанти завдань

Номер варіанта	*VLAN20*			*VLAN30*			*VLAN30*		
	PC2_1	***PC2_1***	***PC2_3***	***PC3_1***	***PC3_2***	***PC3_3***	***PC4_1***	***PC4_2***	***PC4_3***
1	20.0.0.10	20.0.0.11	20.0.0.12	30.0.0.10	30.0.0.11	30.0.0.12	40.0.0.10	40.0.0.11	40.0.0.12
2	20.0.0.20	20.0.0.21	20.0.0.22	30.0.0.20	30.0.0.21	30.0.0.22	40.0.0.20	40.0.0.21	40.0.0.22
3	20.0.0.30	20.0.0.31	20.0.0.32	30.0.0.30	30.0.0.31	30.0.0.32	40.0.0.30	40.0.0.31	40.0.0.32
4	20.0.0.40	20.0.0.41	20.0.0.42	30.0.0.40	30.0.0.41	30.0.0.42	40.0.0.40	40.0.0.41	40.0.0.42
5	20.0.0.50	20.0.0.51	20.0.0.52	30.0.0.50	30.0.0.51	30.0.0.52	40.0.0.50	40.0.0.51	40.0.0.52
6	20.0.0.60	20.0.0.61	20.0.0.62	30.0.0.60	30.0.0.61	30.0.0.62	40.0.0.60	40.0.0.61	40.0.0.62
7	20.0.0.70	20.0.0.71	20.0.0.72	30.0.0.70	30.0.0.71	30.0.0.72	40.0.0.70	40.0.0.71	40.0.0.72
8	20.0.0.80	20.0.0.81	20.0.0.82	30.0.0.80	30.0.0.81	30.0.0.82	40.0.0.80	40.0.0.81	40.0.0.82
9	20.0.0.90	20.0.0.91	20.0.0.92	30.0.0.90	30.0.0.91	30.0.0.92	40.0.0.90	40.0.0.91	40.0.0.92
10	20.0.0.11	20.0.0.12	20.0.0.13	30.0.0.11	30.0.0.12	30.0.0.13	40.0.0.11	40.0.0.12	40.0.0.13

Запитання та завдання для самоперевірки

1. Для чого використовується стандарт 802.*1Q*?
2. Що таке транк?
3. Для чого використовуються транкові канали?
4. Які команди використовуються для створення віртуальної локальної мережі?
5. Які команди використовуються для призначення порту мережі *VLAN*?
6. Як змінити приналежність портів віртуальної локальної мережі?
7. Як перевірити інформацію про мережу *VLAN*?
8. Опишіть загальні рекомендації з проєктування віртуальної локальної мережі.
9. Наведіть приклади використання віртуальних мереж.
10. Які переваги дає використання віртуальних мереж?
11. На якому рівні модклі *OSI* існують віртуальні мережі *VLAN*?
12. Які проблеми можна вирішти за допомогою *VLAN*?

Лабораторна робота 11
БЕЗДРОТОВІ ТЕХНОЛОГІЇ ТА СТАНДАРТИ ЇХ ПОБУДОВИ

Мета: ознайомитися з основними стандартами бездротових мереж, методами аутентифікації та шифрування.

Основні теоретичні відомості

Поширеним способом організації комп'ютерних мереж є бездротові технології. Основними перевагами їх використання є:

- мобільність;
- масштабованість;
- гнучкість;
- зменшення фінансових витрат;
- швидкість розгортання;
- надійність.

У бездротових технологіях для обміну інформацією між пристроями використовуються радіочастоти (*radio frequency, RF*). За допомогою цієї технології користувачам забезпечено можливість пересування без втрати зв'язку з мережею і без потреби у використанні кабелів з'єднання, характерних для традиційних мережних систем *Ethernet*.

До спектра електромагнітних хвиль входять смуги радіочастот, інфрачервоне та видиме світло, рентгенівське випромінювання й гамма-випромінювання. Кожній з цих смуг відповідає конкретний діапазон довжин хвиль і потужностей. Деякі області спектра виділені для мереж загального користування та можуть використовуватись без обмежень і без необхідності отримання спеціальних дозволів. Для бездротових мереж загального користування зазвичай використовується інфрачервоний спектр і частина радіочастотного діапазону.

Робота бездротових мережних пристроїв базується на використанні випромінювання радіочастот у діапазонах 900 МГц, 2,4 ГГц і 5 ГГц.

Бездротові мережі поділяються на три основні категорії:

- бездротові персональні мережі (*Wireless Personal Area network, WPAN*);

- бездротові локальні мережі (*Wireless Local Area network, WLAN*);
- бездротові глобальні мережі (*Wireless Wide Area network, WWAN*).

Інститут інженерів з електротехніки та електроніки *IEEE* є некомерційною загальносвітовою установою, яка переймається реалізацією та постійною розробкою набору стандартів технологій бездротового обміну даними. Набір цих стандартів відомий під назвою *IEEE 802.11*, він складається з самих стандартів та протоколів, які визначають способи обміну даними за допомогою *WLAN*.

Розвиток галузей бездротового обміну даними у локальних мережах та радіообміну регулюється декількома установами. Ці установи розробляють та впроваджують стандарти та приписи, які накладають обмеження на параметри зв'язку, зокрема вихідну потужність, висоту антен, сумісність обладнання, виділення та використання радіочастот та загальне керування діапазоном зв'язку.

Так *ITU-R* регулює міжнародний розподіл радіодіапазонів та орбіт супутників. Основою метою роботи цієї установи є запобігання спільному використанню каналів операторами зв'язку.

Wi-Fi Alliance підтримує рівень сумісності технологій. Своє завдання організація виконує шляхом сертифікації продукції різних виробників.

IEEE – Інститут інженерів з електротехніки та електроніки, це спільнота професіоналів, що працює над покращенням технологій, «сприяє технологічним розробкам та їх удосконаленню для потреб всього людства».

Для забезпечення обміну даними у бездротових локальних мережах потрібне певне обладнання. За загальною класифікацією це обладнання можна поділити на передавач, антену і приймач. Можливі також пристрої, які поєднують у собі ці частини обладнання. За допомогою клієнтських перехідних пристроїв (адаптерів) стаціонарні та портативні комп'ютери можуть з'єднуватися і обмінюватися даними у бездротовій локальній мережі. За допомогою антен відбувається поширення сигналу у всіх напрямках. Існує три основних категорії антен бездротових локальних мереж: неспрямовані, напівспрямовані і сильно спрямовані.

Для бездротових мереж розрізняють режими з'єднання – «точка-точка» та «точка доступу». У режимі «точка-точка» обмін дани-

ми здійснюється безпосередньо без потреби у центральній точці керування обміном даними. Типовим і найпоширенішим є режим «точки доступу». У режимі «точка доступу» використовується пристрій бездротової точки доступу (*WAP*), який є центральним пристроєм, що керує передаванням даних між клієнтськими комп'ютерами.

Часто говорять, що пристрої стандартів *802.11b* і *802.11g* (найпоширеніших стандартів) працюють на частоті 2.4 ГГц. Насправді, сигнали таких пристроїв поширюються на одному з одинадцяти окремих проміжків (або каналів) смуги 2,4 ГГц. Подекуди законодавство дозволяє роботу на тринадцяти каналах, але розпорядження Федеральної комісії зі зв'язку США визначають саме одинадцять каналів. Це означає, що ви можете налаштувати ваш адаптер бездротового зв'язку або точку доступу на роботу у трошки іншому діапазоні, ніж інші мережі у вашій місцевості, щоб уникнути взаємних перешкод та перевантаження.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант завдання в табл.11.1.

Таблиця 11.1

Завдання

Номер варіанта	Стандарти бездротових технологій
1	*802.11, 802.11d, 802.11v*
2	*802.11a, 802.11e, 802.11y*
3	*802.11b, 802.11f, 802.11w*
4	*802.11g, 802.11h, 802.11ac*
5	*802.11n, 802.11i, 802.11d*
6	*802.11, 802.11m, 802.11t*
7	*802.11a, 802.11p, 802.11s*
8	*802.11b, 802.11s, 802.11v*
9	*802.11g, 802.11t, 802.11w*
10	*802.11n, 802.11u, 802.11f*

4. Провести порівняльний аналіз указаних у варіанті бездротових технологій за такими параметрами:

- специфікація;
- дата виходу;
- максимальна швидкість;
- частоти (канали);
- радіус дії;
- елементи;
- обладнання;
- типи антен;
- режими з'єднання;
- безпека;
- розмір та структура кадру.

5. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Поясніть, що означає абревіатура *Wi-Fi*. Який номер стандарту вона визначає?
2. Наведіть основні переваги застосування бездротових мереж.
3. Наведіть основні елементи мережі *Wi-Fi*.
4. Наведіть назви трьох класів кадрів, що використовує стандарт *IEEE 802.11*, та поясніть їх загальне призначення.
5. Наведіть структуру інформаційного кадру 802.11 та поясніть призначення його полів.
6. Наведіть основні різновиди стандарту *IEEE* 802.11
7. Охарактеризуйте стандарт *IEEE* 802.11.
8. Дайте стислу характеристику стандарту *IEEE 802.11b*.
9. Охарактеризуйте стандарт *IEEE 802.11g*.
10. Дайте стислу характеристику стандарту *IEEE 802.11a*.
11. Охарактеризуйте стандарт *IEEE 802.11n*.
12. Які діапазони чатсот використовуються для бездоротової мережі?
13. Яке обладнання необхідне для організації бездротової мережі?
14. Назвіть режими з'єднання у бездротових мережах.
15. Що таке режим «точка-точка»?
16. Який радіус дії мають бездротові мережі?

Лабораторна робота 12
АДРЕСАЦІЯ В IP-МЕРЕЖАХ

Мета: ознайомитися з адресацією в *IP*-мережах.

Основні теоретичні відомості

Кожний комп'ютер у мережі *TCP*/*IP* може мати адреси трьох рівнів: локальні, мережні або доменні імена. Локальні (*MAC*-адреси) розглядалися в лабораторній роботі 7. В даній роботі розглянемо мережні, або *IP*-адреси, які використовуються для однозначної ідентифікації вузлів у межах всієї мережі.

IP-адреси є основним типом адрес, на основі яких мережний рівень передає пакети між мережами. Ці адреси (для версії (*IPv4*) складаються з 32 бітів і записуються у вигляді чотирьох октетів, у десятковій системі числення, наприклад: 192.168.7.5.

IP-адреса складається з двох частин – адреси мережі (*net*) і адреси вузла (*host*). Для виділення номерів мережі, підмережі та хоста (вузла) використовується маска підмережі (*subnet mask*) – бітовий шаблон, в якому бітам, що використовуються для адреси підмережі, присвоюються значення 1, а бітам адреси вузла – значення 0.

Так, маска мережі 255.255. 255.0 (11111111 11111111 11111111 00000000) визначає, що поле адреси мережі містить 24 біти, а поле адреси вузла – 8 бітів. Для наведеного вище прикладу адреси це означає: 192.168.7 – мережна частина (адресу мережі прийнято записувати 192.168.7.0), а 5 – адреса вузла в цій мережі.

Існує 5 класів *IP*-адрес (табл.12.1).

Таблиця 12.1

Класи IP-адрес

Клас	Адреси	Максимальна кількість мереж	Максимальна кількість вузлів у мережі
A	1.0.0.0 – 126.0.0.0	2^7-2	2^{24}-2
B	128.0.0.0 – 191.255.0.0.	2^{14}-2	2^{16}-2
C	192.0.0.0 – 223.255.255.0	2^{21}-2	2^8-2
D	224.0.0.0 – 239.255.255.255	-	Багатоадресний
E	240.0.0.0 – 255.255.255.255	-	Зарезервований

Адреси класу *A* призначені для дуже великих мереж. Як ідентифікатор мережі використовується перший октет, решта три октети

ідентифікують адресу вузлів. Мережа 127.0.0.0 є зарезервованою для зворотного петлевого (loopback) тестування (маршрутизатори або локальні вузли можуть використовувати його для передавання пакетів самим собі). Адреса 0.0.0.0 також є зарезервованою.

Адреси класу *B* використовуються для мереж середнього та великого розмірів, перші два октети використовуються для мережної адреси, інші два – для адреси вузла.

Адреси класу *C* – найчастіше використовувані адреси, призначені для використання в малих мережах.

Адреси класу *D* були створені для реалізації в *IP*-адресах механізму багатоадресної розсилки. Багатоадресною або груповою адресою (*multicast address*) називається унікальна мережна адреса, що використовується для відправлення пакетів певним групам мережних пристроїв. Таким чином, одна мережна станція може передавати один потік даних декільком отримувачам. Діапазон адрес класу *D* називають багатоадресними *IP*-адресами і він також певним чином обмежений.

Адреси класу *E* були зарезервовані проблемною групою проєктування *Internet* для власних дослідницьких потреб і не використовуються в мережі *Internet*.

Службові *IP*-адреси наведені в табл. 12.2.

Таблиця 12.2

Службові *IP*-адреси

Адреси	Призначення
0.0.0.0	Обмежена адреса відправника
255.255.255.255	Обмежена широкомовна адреса (*limited broadcast*)
x.x.x.255	Мережна (*підмережна*) широкомовна адреса (*broadcast*)
127.x.x.x	Зарезервовано для програмного інтерфейсу (*loopback*)
10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Діапазони приватних (білих) *IP*-адрес

Білі (*public*, публічні, зовнішні) *IP*-адреси призначаються мережному пристрою для забезпечення прямого доступу по всій мережі Інтернет та часто належать веб-серверам, поштовим серверам і будь-яким серверним пристроям, доступним безпосередньо з глобальної мережі.

Іноді зустрічається запис *IP*-адрес 192.168.5.0/24. Даний вид запису замінює собою вказівку діапазону *IP*-адрес. Число після по-

хилої риски означає кількість одиничних розрядів у масці підмережі.

З ростом мережі Інтернет необхідність у додаткових *IP*-адресах зростає. Вже зараз тієї кількості *IP*-адрес, яка закладена в *IP* версії 4 не вистачає. Тому був розроблений протокол *IP* версії 6.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл.12.3 та для наведених *IP*-адрес визначити, чи можливе призначення даної адреси користувачу.

Таблиця 12.1

Завдання

Номер варіанта	*IP*-адреси				
1	24.36.206.224	216.14.55.255	150.127.221.244	195.234.253.0	224.156.217.73
2	68.234.252.54	244.89.66.214	228.25.151.208	193.57.186.255	61.73.80.249
3	162.248.255.172	127.149.164.184	62.212.191.157	205.174.246.211	85.99.214.46
4	55.53.117.15	183.201.255.255	248.160.213.60	204.148.8.129	157.175.173.101
5	116.63.189.57	11.255.106.92	84.255.157.124	163.91.219.180	192.70.216.255
6	230.186.26.106	107.160.259.220	194.172.47.255	44.33.251.103	127.156.115.223
7	194.129.77.139	243.276.165.176	101.255.42.94	187.150.256.191	116.55.50.117
8	89.155.70.255	192.202.66.255	130.14.216.186	50.159.154.235	246.158.79.190
9	105.104.16.79	208.135.84.111	64.155.234.19	3.165.255.65	197.26.192.255
10	71.166.50.255	198.77.3.22	13.140.114.109	196.153.99.255	127.248.4.219

Якщо неможливе – вказати причину. Для можливих адрес указати:

- клас;
- адресу мережі (*network address*);
- адресу хоста (*host address*);
- маску підмережі (*subnet mask*);
- двійкове значення адреси;
- широкомовну адресу *broadcast*.

4. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Що таке *IP*-адреса?
2. З яких частин складається *IP*-адреса?
3. Які класи *IP*-адрес ви знаєте?
4. Поясніть поняття *loopback*, *broadcast*, *multicast*.
5. Що відбудеться при відправленні пакета за адресою 127.0.0.1?
6. Яку частку всієї безлічі *IP*-адрес становлять адреси класу *A*? Класу *B*? Класу *C*?
7. Дайте визначення маски підмережі.
8. З якою метою використовується маска підмережі?
9. Поясніть, як визначити діапазон номерів мереж класів *IP*-адрес.
10. Як визначити максимальну кількість *IP*-адрес у кожному класі?
11. З якою метою використовуються адреси класів *D* та *E*?
12. Охарактеризуйте особливі *IP*-адреси та поясніть їх призначення.

Лабораторна робота 13
РОЗБИТТЯ МЕРЕЖІ НА ПІДМЕРЕЖІ

Мета: ознайомитися з методикою розбиття мережі на підмережі, розрахувати число підмереж та вузлів за префіксом підмережі.

Основні теоретичні відомості

Альтернативою традиційній схемі поділу *IP*-адрес на номер мережі та номер вузла (базується на понятті класу) є використання маски, за допомогою якої можна більш гнучко встановлювати межу між номером мережі та номером хоста (вузла). Якщо для позначення маски застосовується запис із «/» (префіксом), наприклад 129.54.65.3/16, то це означає, що маска для адреси 129.54.65.3 містить 16 одиниць, тобто під номер мережі відведено 16 двійкових розрядів (перші 2 байти).

В основу механізму масок покладено принцип отримання номера мережі шляхом порозрядного перемноження адреси вузла і маски. Наприклад, для *IP*-адреси 180.34.23.134 з маскою 255.255.0.0 маємо мережу 180.34.0.0.

Супроводжуючи кожну *IP*-адресу маскою, можна відмовитися від понять класів і адрес та зробити гнучкою систему адресації. Наприклад, якщо адресу 129.54.170.164 асоціювати з маскою

255.255.255.0, то номером мережі буде 129.54.170.0 (а не 129.54.0.0 як це визначено системою класів).

Для виділення підмережі частина бітів, що відповідає за нумерацію вузла, може бути визначена як мережна. Такий механізм називають запозиченням (орендою) бітів. Процес ділення завжди починається з крайнього лівого біта вузла, положення якого залежить від класу *IP*-адреси. Вибір необхідної кількості бітів для створення підмережі залежить від потрібної максимальної кількості її вузлів.

Використання масок змінної довжини (*VLSM – Variable Length Subnet Masking*) заощаджує використання адресного простору. Основна ідея полягає в обчисленні маски окремо для кожної підмережі.

Можлива кількість підмереж обчислюється як $N=2^n$, де n – кількість позичених з хостової частини бітів, можлива кількість хостів в підмережі: $H=2^m-2$, де m – кількість бітів хостової частини, що лишилась. Початкова кількість бітів хостової частини: $m+n$.

Розглянемо приклад розбиття мережі 74.126.205.0 з маскою 255.255.255.0 на 4 однакові підмережі. Порахуємо кількість бітів в основній масці, що необхідні для створення підмереж: оскільки мереж потрібно 4, тобто 2^2, то буде позичено 2 біти в основній масці мережі:

74.126.205.0 – 01001010.01111110.11001101.00000000

255.255.255.192 – 11111111.11111111.11111111.**11000000**.

Розширення маски до значення 255.255.255.192 відбулося за рахунок двох позичених бітів у початковій частині хоста в адресі, які були використані для створення підмереж. Ідентифікатор хоста тепер містить шість бітів, тому кожна підмережа може містити $2^6-2=62$ адрес хостів (нагадаємо, адреси хостів не можуть складатися тільки з нулів або одиниць).

Слід зазначити, що чим більше бітів використовується для маски підмережі, тим більше доступно підмереж. Однак, чим більше підмереж можна створити, тим менше адрес хостів в них буде. Створені підмережі наведені в табл. 13.1.

Розглянемо ще один приклад, коли задану мережу 74.126.205.0 з маскою 255.255.255.0 необхідно поділити на 4 підмережі з такою кількістю хостів у кожній підмережі: 14,28,15,5. Визначимо, яку

маску необхідно використати, щоб отримати необхідну кількість хостів.

Таблиця 13.1

Мережа в десятковій та двійковій системі числення

Підмережі в десятковій системі числення	Підмережі в двійковій системі числення
74.126.205.0	01001010.01111110.11001101.**00**000000
74.126.205.64	01001010.01111110.11001101.**01**000000
74.126.205.128	01001010.01111110.11001101.**10**000000
74.126.205.192	01001010.01111110.11001101.**11**000000
Маска підмережі	Маска підмережі
255.255.255.192	11111111.11111111.11111111.11000000

Підмережа 1: необхідно 14 хостів, найближче значення 2^n=16, тобто кількість бітів хостової частини n=4, кількість бітів для ідентифікатора підмережі буде 8-4=4. Відповідно маска цієї підмережі буде 255.255.255.240 або /28.

Підмережа 2: необхідно 28 хостів, найближче значення 2^n=32, тобто кількість бітів хостової частини n=5, кількість бітів для ідентифікатора підмережі буде 8-5=3. Відповідно маска цієї підмережі буде 255.255.255.224 або /27.

Підмережа 3: необхідно 15 хостів, найближче значення 2^n=16, але потрібно врахувати ще й широкомовну адресу та адресу підмережі, тому 16 бітів буде недостатньо для даної підмережі. Відповідно вибираємо 2^n=32, тобто кількість бітів хостової частини n=5, кількість бітів для ідентифікатора підмережі буде 8-5=3. Відповідно маска цієї підмережі буде 255.255.255.224 або /27.

Підмережа 4: необхідно 5 хостів, найближче значення 2^n=8, тобто кількість бітів хостової частини n=3, кількість бітів для ідентифікатора підмережі буде 8-3=5. Відповідно маска цієї підмережі буде 255.255.255.248 або /29.

У разі розбиття мережі методом *VLSM*, вона спочатку розбивається на підмережі, а потім знову ділиться на підмережі. Спочатку відсортуємо мережі за кількістю доступних хостів:

Підмережа 2: 32 хоста;

Підмережа 3: 32 хоста;

Підмережа 1: 16 хостів;

Підмережа 4: 8 хостів.

Далі розбиваємо задану мережу (в якій доступно 256 адрес) по 32 адреси (найбільша задана підмережа). В утворених підмережах кількість бітів ідентифікаторів дорівнює 3, значить нові підмережі будуть виглядати наступним чином:

01001010.01111110.11001101.**000**00000
01001010.01111110.11001101.**001**00000
01001010.01111110.11001101.**010**00000
01001010.01111110.11001101.**011**00000
01001010.01111110.11001101.**100**00000
01001010.01111110.11001101.**101**00000
01001010.01111110.11001101.**110**00000
01001010.01111110.11001101.**111**00000

Нам необхідні лише перші дві підмережі (для підмереж 2 та 3), їх маска 255.255.255.224 або /27.

Для визначення наступної підмережі ділимо мережу 01001010.01111110.11001101.**010**00000 пополам (тобто позичаємо ще один біт), отримуємо дві підмережі:

01001010.01111110.11001101.**0100**0000
01001010.01111110.11001101.**0101**0000

Першу з них відводимо для підмережі 1 з маскою /28. Другу нову ділимо пополам (позичаємо ще один біт):

01001010.01111110.11001101.**01010**000
01001010.01111110.11001101.**01011**000

Першу з них відводимо для підмережі 4 з маскою /29.

Для визначення діапазону можливих хостів для кожної підмережі, необхідно спочатку до номера підмережі додати одиницю (це буде номер першого хоста), а потім до номера підмережі додати кількість можливих адрес (це буде адреса останнього хоста):

Підмережа 2: 74.126.205.1 - 74.126.205.30
Підмережа 3: 74.126.205.33 - 74.126.205.62
Підмережа 1: 74.126.205.65 - 74.126.205.78
Підмережа 4: 74.126.205.81 - 74.126.205.86.

Результат переведення значень знайдених підмереж наведено в табл. 13.2.

Таблиця 13.2

Параметри підмереж

Підмережі	Підмережі в двійковій системі числення	Підмережі в двійковій системі числення	Маска
2	01001010.01111110.11001101.**000**00000	74.126.205.0	255.255.255.224
3	01001010.01111110.11001101.**001**00000	74.126.205.32	255.255.255.224
1	01001010.01111110.11001101.**0100**0000	74.126.205.64	255.255.255.240
4	01001010.01111110.11001101.**01010**000	74.126.205.80	255.255.255.248

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл.13.3 та виконати розбиття мережі на 4 однакові підмережі.

Таблиця 13.3

Завдання

Номер варіанта	Розбиття на однакові підмережі		Розбиття на різні підмережі		
	Адреса мережі	Маска	Адреса мережі	Маска	Кількість хостів в підмережах
1	129.138.60.0	255.255.252.0	126.198.0.0	255.254.0.0	155, 255, 86, 161
2	13.140.208.0	255.255.240.0	192.200.0.0	255.248.0.0	72, 104, 130, 109
3	109.88.38.0	255.255.254.0	10.192.0.0.	255.252.0.0	73, 55, 133, 106
4	48.185.104.0	255.255.248.0	156.168.0.0	255.248.0.0	92, 180, 105, 102
5	144.29.236.0	255.255.252.0	81.176.0.0	255.248.0.0	89, 158, 171, 60
6	78.97.205.0	255.255.255.0	91.184.0.0	255.252.0.0	80, 100, 64, 159
7	192.199.140.0	255.255.252.0	190.128.0.0	255.254.0.0	99, 63, 155, 61
8	87.247.176.0	255.255.240.0	65.48.0.0	255.248.0.0	120, 130, 92, 145
9	191.197.206.0	255.255.254.0	125.192.0.0	255.240.0.0	65, 94, 59, 189
10	17.53.208.0	255.255.248.0	14.160.0.0	255.224.0.0	50, 258, 140, 107

Для кожної з підмереж указати:

- мережну адресу підмережі;
- маску підмережі;
- префікс маски підмережі;

- широкомовну адресу підмережі;
- діапазон доступних адрес хостів в підмережі;
- кількість вузлів мережі.

4. Виконати розбиття мережі на 4 різні підмережі. Для кожної з підмереж вказати:
   - мережу адресу підмережі;
   - маску підмережі;
   - префікс маски підмережі;
   - широкомовну адресу підмережі;
   - діапазон доступних адрес хостів в підмережі;
   - кількість вузлів мережі.
5. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Навіщо потрібна мережна адреса?
2. В чому різниця між безкласовою та класовою адресацією?
3. Що покладено в основу механізму масок підмережі?
4. Які форми запису маски ви знаєте?
5. У чому суть методу *VLSM*?
6. Чи можна в локальній мережі застосовувати *VLSM*?
7. Яка максимальна довжина маски у разі використання *VLSM*?
8. Як *VLSM* допомагає економному використанню адресного простору?
9. Поясність суть запозичення (оренди бітів).
10. Як обчислюється можлива кількість підмереж?
11. Як обчислюється можлива кількість хостів в підмережі?
12. Які ви знаєте правила для визначення мережної адреси вузла?
13. Як можна визначити адресу першого та останнього вузла підмережі?
14. Опишіть метод розбиття мережі на рівні підмережі.
15. Яке значення має маска підмережі під час аналізу *IP*-адреси?

Лабораторна робота 14
ДІАГНОСТИКА IP-ПРОТОКОЛУ

Мета: ознайомитись з мережними налаштуваннями операційної системи *Windows*.

Основні теоретичні відомості

Існують різні утиліти, що дозволяють швидко продіагностувати *IP*-підключення. Більшість операцій легко може бути виконана з використанням команд самої операційної системи. *Windows* також має інтерфейс командного рядка (*CLI*, «консоль»), cmd.exe. Докладнішу загальну інформацію можна отримати, набравши в командному рядку «*help*» для отримання загальних відомостей про доступні команди та «ім'я команди /?». Інтерфейс командного рядка доступний як у вигляді вікна, так і в повноекранному вигляді (перемикання між ними здійснюється натисненням *Alt+Enter*).

Ipconfig – утиліта, що використовується для відображення налаштувань всіх мережних адаптерів: значення адреси, маски, шлюзу. Щоб побачити результат виконання, потрібно в командному рядку ввести *ipconfig*. Якщо ввести *ipconfig /all*, то результатом буде повна конфігурація *TCP*/*IP* для всіх адаптерів.

Утиліта *ipconfig* підтримує декілька параметрів командного рядка, доступні варіанти можна переглянути, ввівши ipconfig /?.

Ping – утиліта, що відправляє запити *Echo-Request* протоколу *ICMP* зазначеному вузлу мережі й фіксує відповіді (*ICMP Echo-Reply*). Час між відправленням запиту й одержанням відповіді (*RTT*, від англ. *Round Trip Time*) дозволяє визначати двосторонні затримки (*RTT*) у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

Повна відсутність *ICMP*-відповідей може також означати, що віддалений вузол (або якийсь із проміжних маршрутизаторів) блокує *ICMP Echo-Reply* або ігнорує *ICMP Echo-Request*. Програма *ping* є одним з основних діагностичних засобів у мережах *TCP*/*IP* і входить у поставку всіх сучасних мережних операційних систем. Функціональність *ping* також реалізована в деяких вбудованих ОС маршрутизаторів, доступ до результатів виконання *ping* для таких пристроїв за протоколом *SNMP* визначається *RFC 2925* (*Definitions*

of *Managed Objects for Remote Ping, Traceroute, and Lookup Operations*).

Практичне застосування:

- можна дізнатися *IP*-адресу за доменним ім'ям;
- можна перевірити, чи є зв'язок із сервером;
- перевірити якість каналу, подивившись, скільки пакетів не дійшло або час відклику.

Синтаксис команди: ping *IP*-adress /*URL*, де замість *IP*-адрес /*URL* потрібно ввести *IP*-адресу вузла, до якого перевіряється з'єднання чи адресу веб-вузла. Наприклад, *ping* 72.163.4.185 або *ping cisco.com* (рис.14.1).

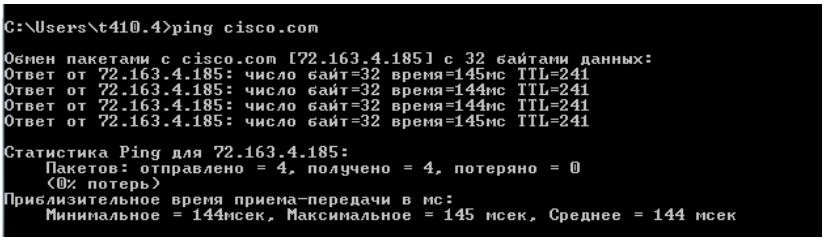

Рис. 14.1. Перевірка з'єднання

Утиліта *ping* має ряд параметрів:

-t Відправка пакетів на вказаний вузол до команди переривання
-a Встановлення адреси за іменами вузлів
-n Кількість запитів, що відсилаються
-l Розмір буфера відсилання
-f Встановлення прапорця, що забороняє фрагментацію пакета
-i Встановлення строку життя пакета <"*Time To Live*">
-v Встановлення типу служби <"*Type Of Service*">
-r Запис маршруту для вказаної кількості переходів
-s Штамп часу для вказаної кількості переходів
-j Вільний вибір маршруту за списком вузлів
-k Жорсткий вибір маршруту по списку вузлів
-w Таймаут кожної відповіді в мілісекундах

Tracert – утиліта, призначена для визначення маршрутів прямування даних в мережах *TCP/IP*. Traceroute може використовувати різні протоколи передавання даних залежно від операційної системи пристрою. Такими протоколами можуть бути *UDP*, *TCP*, *ICMP*

або *GRE*. Комп'ютери зі встановленою операційною системою Windows використовують *ICMP* протокол, при цьому маршрутизатори *Cisco* - протокол *UDP*. Синтаксис команди: *tracert IP*-adress |*URL*, де замість *IP*-adress |*URL* потрібно ввести *IP*-адресу вузла, до якого перевіряється з'єднання чи адресу веб-вузла. Наприклад, *tracert* 72.163.4.185 або *tracert cisco.com* (рис.14.2).

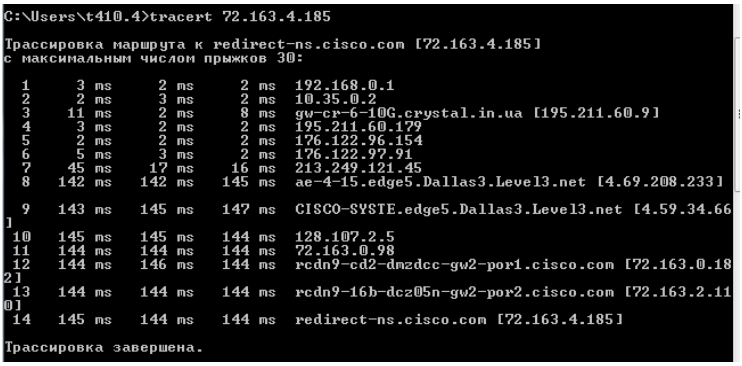

Рис. 14.2. Визначення маршруту

ARP (*Address Resolution Protocol*) – протокол визначення адрес, комунікаційний протокол, призначений для перетворення *IP*-адрес (адрес мережного рівня) в *MAC*-адреси (адреси канального рівня) в мережах *TCP*/*IP*.

Існують такі типи повідомлень *ARP*: запит *ARP* (*ARP* request) і відповідь *ARP* (*ARP* reply). Система-відправник за допомогою запиту *ARP* запитує фізичну адресу системи-одержувача. Відповідь (фізичну адресу вузла-одержувача) приходить у вигляді відповіді *ARP*. Перед тим як передати пакет мережного рівня через сегмент *Ethernet*, мережний стек перевіряє кеш *ARP*, щоб з'ясувати, чи не зареєстрована в ньому вже потрібна інформація про вузол-одержувач. Якщо такого запису в кеші *ARP* немає, то виконується широкомовний запит *ARP*. Цей запит для пристроїв в мережі має наступний зміст: «Хто-небудь знає фізичну адресу пристрою, який володіє такою *IP*-адресою?» Коли одержувач з цією *IP*-адресою прийме цей пакет, то повинен буде відповісти: «Так, це моя *IP*-адреса. Моя фізична адреса….». Після цього відправник оновить свій кеш *ARP* і буде здатний передати інформацію одержувачу.

Щоб переглянути всю *ARP*-таблицю, слід ввести *arp –a*.

Записи в кеші *ARP* можуть бути статичними і динамічними. Приклад, що наведений вище, описує динамічний запис кешу. Можна також створювати статичні записи в таблиці *ARP*. Це можна зробити за допомогою команди:

arp-s <*IP*-адреса> <*MAC*-адреса>

Записи в таблиці *ARP*, створені динамічно, залишаються в кеші протягом двох хвилин. Якщо протягом цих двох хвилин сталася повторна передача даних за цією адресою, то час зберігання запису в кеші продовжується ще на 2 хв. Ця процедура може повторюватися доти, поки запис в кеші проіснує до 10 хв. Після цього запис буде видалено з кешу і буде відправлений повторний запит *ARP*.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант у табл.14.1 та виконати дослідження утиліт *ipconfig, ping, tracert, arp, pathping, getmac, netstat, nslookup*.
4. Для кожної з утиліт навести її опис, параметри, результати виконання із зміненими параметрами.
5. Оформити звіт за результатами виконаої роботи.

Таблиця 14.1

Завдання

Номер варіанта	*IP*-адреси для перевірки утиліт	*URL* адреси для перевірки утиліт
1	216.58.214.238	*google.com*
2	193.178.34.21	*nau.edu.ua*
3	23.185.0.1	*harvard.edu*
4	128.232.132.8	*cam.ac.uk*
5	151.101.2.216	*ox.ac.uk*
6	171.67.215.200	*stanford.edu*
7	151.101.2.133	*yale.edu*
8	155.198.64.149	*imperial.ac.uk*
9	77.47.133.211	*kpi.ua*
10	176.32.103.205	*amazon.com*

Запитання та завдання для самоперевірки

1. Поясність призначення утиліти *ipconfig*.
2. Наведіть приклади параметрів утиліти *ipconfig*, що вони означають?
3. Поясність призначення утиліти *ping*.
4. Які параметри доступні для утиліти ping?
5. З якою метою використовують утиліту *tracert*?
6. Назвіть основні параметри утиліти *tracert*.
7. З якою метою використовують *ARP*-протокол?
8. Які типи повідомлень *ARP* ви знаєте?
9. Яку команду слід ввести в рядку *CLI* для перегляду таблиці *ARP*?
10. Наведіть приклади статичного та динамічного запису в таблиці *ARP*.

Лабораторна робота 15
НАЛАШТУВАННЯ МЕРЕЖНОГО СЕРВІСУ DHCP

Мета: ознайомитись з протоколом *DHCP* та принципом його функціонування.

Основні теоретичні відомості

Присвоєння кожному пристрою *IP*-адреси власноруч є складною проблемою, тому доцільно це зробити автоматично. Для цього використовується протокол під назвою *DHCP*.

Dynamic Host Configuration Protocol (*DHCP*) – протокол, який передбачає механізм автоматичного присвоєння інформації про *IP*-адресу, маску, шлюз та перелік адрес *DNS*-серверів.

Це найбільш бажаний спосіб привласнення *IP*-адрес вузлам у великій мережі, оскільки він полегшує роботу фахівців служби підтримки і практично усуває можливість помилки. Крім того, адреси присвоюються вузлам тимчасово і якщо вузол вимикається або йде з мережі, його адреса повертається в пул для повторного використання.

Під час першого налаштування як клієнта *DHCP* у вузла немає *IP*-адреси, маски підмережі та стандартного шлюзу. Він отримує ці дані за наступною схемою:

- клієнт, якому потрібна *IP*-адреса, посилає повідомлення про пошук *DHCP* у вигляді широкомовної розсилки з *IP*-адресою одержувача 255.255.255.255 (32 одиниці) та *MAC*-адресою одержувача *FF-FF-FF-FF-FF-FF* (48 одиниць);
- кадр *DHCP* отримають всі вузли в мережі, але відповідає тільки сервер *DHCP* який відправляє клієнту запропоновану *IP*-адресу;
- клієнт у відповідь посилає на вказаний сервер запит *DHCP* з підтвердженням використання *IP*-адреси;
- сервер надсилає підтвердження.

DHCP-сервер може знаходитися в іншій мережі, якщо проміжні маршрутизатори сконфігуровані на пересилання *DHCP*-запитів. Крім повідомлень, необхідних для початкового отримання *IP*-адреси клієнтом, *DHCP* передбачає декілька додаткових повідомлень.

Відмова *DHCP*. Якщо після отримання підтвердження від сервера клієнт виявляє, що вказана адреса вже використовується в мережі, він розсилає широкомовне повідомлення відмови *DHCP,* після чого процедура отримання *IP*-адреси повторюється.

Повідомлення відмови *DHCP*. У разі отримання такого повідомлення, клієнт повинен повторити процедуру отримання адреси.

Звільнення *DHCP*. Якщо клієнт хоче зупинити оренду *IP*-адреси, то він надсилає повідомлення про звільнення *DHCP* на той сервер, який давав йому адресу в оренду. Таке повідомлення не є широкомовним.

Інформація *DHCP*. Таке повідомлення використовується для визначення додаткових параметрів *TCP*/IP тими клієнтами, адреса яких налаштована вручну. Сервери відповідають на такий запит повідомленням підтвердження без виділення *IP*-адреси.

Розглянемо налаштування *DHCP* в *Cisco Packet Tracer* на прикладі мережі на рис.15.1.

Для маршрутизатора необхідно додати один *Gigabit Ethernet*-модуль *PT-ROUTER-NM-1CGE*. Для цього відкриємо налаштування маршрутизатора, на вкладці *Physical* на моделі маршрутизатора натиснемо на кнопку живлення, виберемо вказаний модуль, встановимо у вільний слот та ввімкнемо маршрутизатор.

Виконаємо налаштування елементів мережі. Зарезервуємо для маршрутизатора першу доступну *IP*-адресу, для сервера – другу, а

стаціонарним комп'ютерам будемо задавати адреси послідовно з третьої доступної адреси. Мережна маска для всіх пристроїв – 255.255.255.0. Мережа має адресу 192.168.1.0.

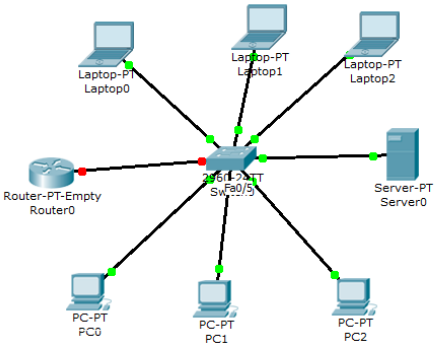

Рис. 15.1 Схема мережі

Для *PC0* на вкладці *Desktop* виберемо пункт *IP Configuration*, режим отримання *IP-адреси Static*, *IP Address* – 192.168.1.3, *Subnet Mask* 255.255.255.192, *Default Gateway* – 192.168.1.1 (перша доступна адреса, що зарезервована для роутера). Решту стаціонарних комп'ютерів налаштовуємо аналогічно.

Налаштуємо маршрутизатор. Для інтерфейсу *GigabitEthernet0*/0 введемо значення *IP*-адреси 192.168.1.1, *Subnet Mask* 255.255.255.0. Після чого включимо даний модуль - *Port Status* встановимо в *On*.

Налаштуємо сервер. Для інтерфейсу *FastEthernet* встановимо *IP*-адресу 192.168.1.2, *Subnet Mask* 255.255.255.0. Потім ввімкнемо даний модуль – *Port Status* встановимо в *On*. Далі налаштуємо *DHCP*. Перейдемо на вкладку Services, підменю *DHCP*. Для вмикання включимо перемикач *Service* в положення On. Назначимо ім'я пулу для роздачі адрес – в поле *Pool Name* введемо *APP_Pool*. В полі *Default Gateway* вкажемо *IP*-адресу роутера 192.168.1.1. Автоматичне призначення *IP*-адрес встановимо з шостої доступної адреси мережі – в поле *Start IP Address* введемо 192.168.1.6, *Subnet Mask* 255.255.255.0. Після натискаємо на *Add*, та в *DHCP*-таблиці з'явиться відповідний запис.

Тепер налаштуємо ноутбуки на автоматичне отримання *IP*-адрес. Відкриємо властивості *Laptop0*, на вкладці *Desktop* виберемо пункт *IP Configuration* та активуємо режим отримання *IP*-адреси

DHCP. Через деякий час в полях *IP Address* та *Subnet Mask* з'являться мережні параметри. В даному випадку це перша *IP*-адреса з доступних для автоматичного присвоєння – 192.168.1.6 та мережна маска 255.255.255.0. Аналогічно налаштовуємо решту ноутбуків. Перевірити назначені адреси можна за допомогою інструмента *Inspect*/*Port Status Summary Table*. Щоб перевірити працездатність мережі, необхідно відправити *ping* запити між її пристроями.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл.15.1 та побудувати мережу, яка буде складатися з маршрутизатора, сервера та 10 *PC* та 10 *Laptop*, що під'єднані до комутатора.
4. Призначити статичну адресу маршрутизатору (перша доступна адреса мережі) та сервера (друга доступна адреса мережі).
5. На сервері налаштувати *DHCP*.
6. Налаштувати на *PC* та *Laptop* динамічне отримання *IP*-адрес. Перевірити працездатність мережі.
7. Оформити звіт за результатами виконаної роботи.

Таблиця 15.1

Завдання

Номер варіанта	Адреса мережі	Маска мережі
1	44.16.105.0	255.255.255.128
2	45.16.115.0	255.255.255.192
3	46.16.125.0	255.255.255.224
4	47.16.135.0	255.255.255.128
5	48.16.145.0	255.255.255.192
6	49.16.155.0	255.255.255.224
7	50.16.165.0	255.255.255.128
8	51.16.175.0	255.255.255.192
9	52.16.185.0	255.255.255.224
10	53.16.195.0	255.255.255.128

Запитання та завдання для самоперевірки

1. Що таке *DHCP*?
2. Для чого використовують *DHCP*?
3. Які етапи отримання *IP*-адреси клієнтом від сервера *DHCP*?
4. Які повідомлення передбачає *DHCP* для виконання задач, не пов'язаних з отриманням *IP*-адреси?
5. Які налаштування необхідно зробити на сервері для *DHCP*?
6. Як перевірити *DHCP* налаштування?

Лабораторна робота 16
НАЛАШТУВАННЯ DHCP НА МАРШРУТИЗАТОРІ CISCO

Мета: ознайомитись з налаштуванням *DHCP* на маршрутизаторі *Cisco*.

Основні теоретичні відомості

Налаштування *DHCP* можна виконати і на маршрутизаторі, якщо мережа невелика. Побудуємо для прикладу мережу (рис.16.1).

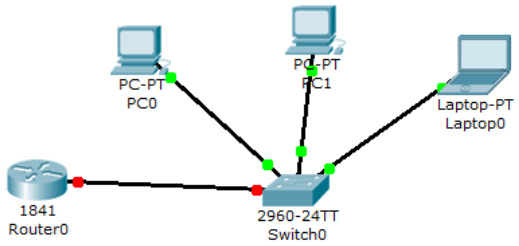

Рис. 16.1. Схема мережі

Налаштуємо маршрутизатор. Введемо наступні команди:

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#in fa0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#ex

Бачимо, що порт загорівся зеленим кольором. Далі створимо пул адрес на *Cisco DHCP server*, для чого введемо команду:

Router(config)#ip dhcp pool DHCP_192.168.1.0

Спочатку вкажемо мережу:

Router(dhcp-config)# network 192.168.1.0 255.255.255.0

Вказуємо шлюз за замовчуванням та DNS сервер:

Router(dhcp-config)#default-router 192.168.1.1

Router(dhcp-config)#dns-server 192.168.1.2

Виключимо з пулу перші 50 адрес, які залишимо для серверів та про запас:

Router(dhcp-config)#ip dhcp excluded-address 192.168.1.1 192.168.1.50

Router(config)#do wr mem

Перевіримо налаштування на *PC0*. Якщо в командному рядку ввести команду ipconfig, щоб подивитися поточні налаштування, то побачимо, що *IP*-адреса не налаштована. На вкладці *Desktop* виберемо пункт *IP Configuration* та активуємо режим отримання *IP*-адреси *DHCP*. Через деякий час в полях *IP Address* та *Subnet Mask* з'являться мережні параметри. Повторно в командному рядку введемо *ipconfig*. Як бачимо, *IP*-адреса отримана (рис.16.2).

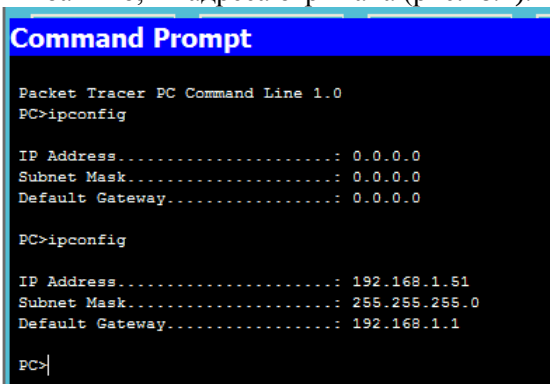

Рис. 16.2 Схема мережі

На *PC1* та *Laptop0* зробимо аналогічні налаштування. Для тестування працездатності мережі скористаємося утилітою *ping*.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл.16.1.

Таблиця 16.1

Завдання

Номер варіанта	Адреса мережі	Маска мережі
1	49.16.155.0	255.255.255.224
2	50.16.165.0	255.255.255.128
3	51.16.175.0	255.255.255.192
4	52.16.185.0	255.255.255.224
5	53.16.195.0	255.255.255.128
6	44.16.105.0	255.255.255.128
7	45.16.115.0	255.255.255.192
8	46.16.125.0	255.255.255.224
9	47.16.135.0	255.255.255.128
10	48.16.145.0	255.255.255.192

4. Побудувати мережу (рис.16.3).

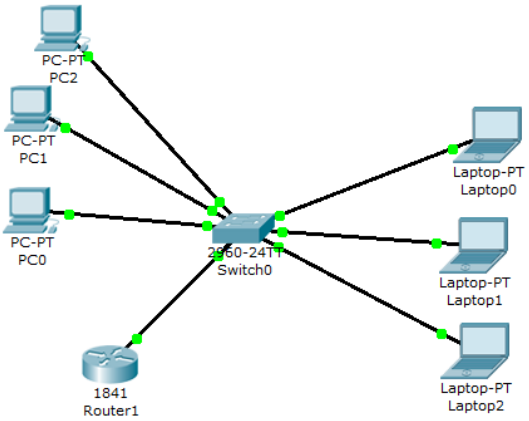

Рис. 16.3. Схема мережі до завдання

5. Налаштувати *DHCP* на маршрутизаторі.
6. Налаштувати на *PC* та *Laptop* динамічне отримання *IP*-адрес. Перевірити працездатність мережі.
7. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Для чого використовується *DHCP* на маршрутизаторі?
2. Як налаштувати *DHCP* на маршрутизаторі *Cisco*?
3. Які команди використовуються для налаштувань *DHCP*?
4. Як налаштувати пул адрес?
5. Як вилучити певні адреси із видачі?

Лабораторна робота 17
НАЛАШТУВАННЯ HTTP ТА DNS-СЕРВЕРІВ В CISCO PACKET TRACER

Мета: ознайомитись з особливостями функціонування та налаштуванням *HTTP* та *DNS*-серверів в *Cisco Packet Tracer*.

Основні теоретичні відомості

Як правило, сервер віддає в мережу свої ресурси, а клієнт ці ресурси використовує. Також на серверах встановлюють спеціалізоване програмне і апаратне забезпечення. На одному комп'ютері одночасно може бути встановлено декілька серверів.

Cisco HTTP (*Web*) сервер дозволяє створювати найпростіші вебсторінки і перевіряти проходження пакетів на 80й порт сервера. Ці сервери надають доступ до вебсторінок, супутніх ресурсів.

DNS сервер дозволяє перетворювати доменні імена серверів в *IP*-адреси. *DNS* (*Domain Name System*, система доменних імен) – це система для отримання інформації про домени. Розподілена база даних *DNS* підтримується за допомогою ієрархії *DNS*-серверів, що взаємодіють за певним протоколом. Основою *DNS* є уявлення про ієрархічну структуру доменного імені та зонах. Домен – це вузол в дереві імен, разом із підпорядкованими йому вузлами (якщо такі є), тобто іменована гілка або піддерево в дереві імен. Доменне ім'я читається зліва направо від молодших доменів до доменів вищого рівня: зверху знаходиться кореневий домен, нижче ідуть домени

першого рівня, потім другого рівня і т.д. Наприклад, для адреси *ua.wikipedia.org* домен першого рівня – *org*, другого – *Wikipedia*, третього – *ua*.

Теоретично, такий поділ може досягати глибини 127 рівнів, а кожна мітка складатися з 63 символів, поки загальна довжина доменного імені не досягне 254 символів разом з крапками. Але на практиці регістратори доменних імен використовують більш жорсткі обмеження до 2 – 3 рівнів.

Слід зазначити, що *DNS* ім'я та *IP*-адреси не тотожні, оскільки одна IP-адреса може мати багато імен, що дозволить підтримувати на одному комп'ютері багато веб-сайтів.

Розглянемо налаштування *Web*-сервера в *Cisco Packet Tracer*. Побудуємо мережу (рис.17.1), виконаємо базові налаштування *IP*-адрес.

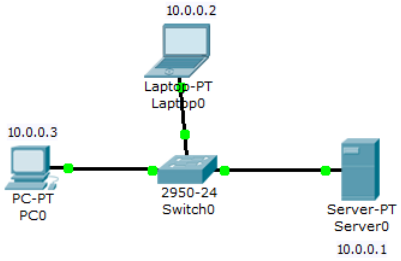

Рис. 17.1. Схема мережі

Для створення *HTTP*-сервера відкриваємо на сервері вкладку *HTTP* і редагуємо першу сторінку сайту з назвою *index.html*. Ввмикаємо службу *HTTP* перемикачем *On* (рис.17.2).

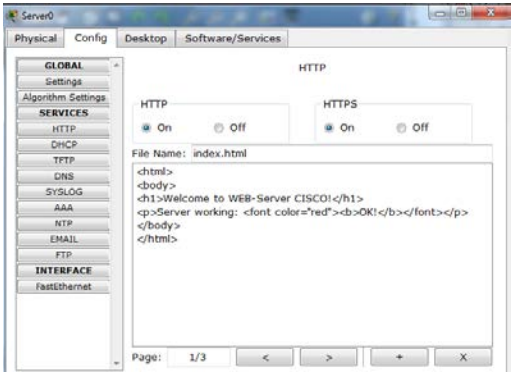

Рис. 17.2. Вкладка *Config*, служба сервера *HTTP*

У цьому вікні можна додати нову сторінку кнопкою «+» або видалити поточну кнопкою «X». Перемикання між кількома сторінками здійснюється кнопками < >. У вікні *html* коду створюємо текст першої сторінки сайта *index.html*. Текст можна переносити через буфер обміну. Він може бути тільки англійською мовою:

```
<html>
<body>
<h1>Welcome to WEB-Server CISCO!</h1>
<p>Server working: <font color="red"><b>OK!</b></font></p>
</body>
</html>
```

На другій сторінці *page2.html* вписуємо такий код:

```
<html>
<center><font size='+2' color='blue'>Welcome to Cisco Packet Tracer HTML
Server! </font></center>
<body>
Hello!<br/>I am OK!
</body>
</html>
```

На третій сторінці *page3.html*:

```
<html>
<body>
<center><font size='+2' color='red'>This is Computer Networks Laboratory Tutorial</font></center>
<p></p>
</body>
</html>
```

Щоб перевірити працездатність сервера, відкриваємо клієнтську машину (10.0.0.2 або 10.0.0.3) і на вкладці *Desktop* (Робочий стіл) запускаємо додаток *Web Browser*. Після чого набираємо адресу вебсервера 10.0.0.1 і натискаємо на кнопку *GO*. Переконуємося, що він працює.

По черзі переглядаємо сторінки http://10.0.0.1/page2.html та http://10.0.0.1/page3.html (рис. 17.3).

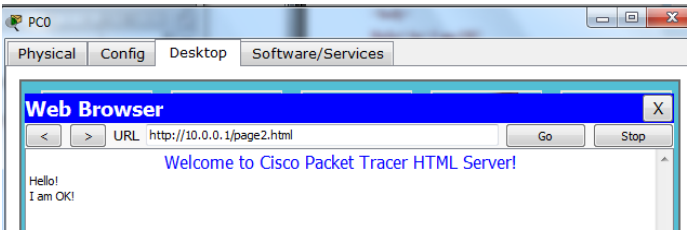

Рис. 17.3. Текст вебсторінки

Змінимо конфігурацію мережі (рис.17.4), налаштуємо на *Server0 DNS*, а на *Server1 DHCP*.

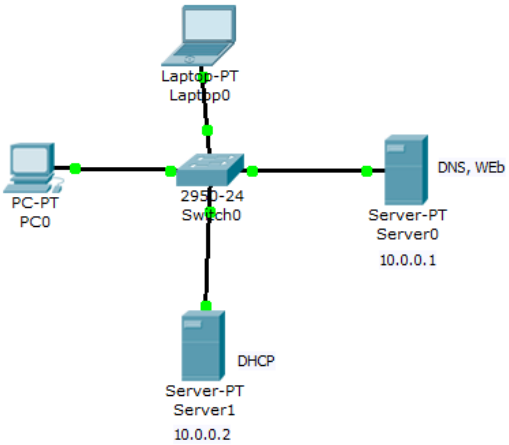

Рис. 17.4. Конфігурація мережі

На *PC0* та *Laptop0* необхідно встановити налаштування *IP*-адрес через DHCP. У конфігурації *Server0* виберемо вкладку *DNS* і задамо два ресурсні записи (*Resource Records*) в прямій зоні *DNS*.

Спочатку для запису типу *A Record* вкажемо доменне ім'я комп'ютера *server0.mysite.ua* та його *IP*-адресу 10.0.0.1, натиснемо на кнопку *Add* (додати) і активуємо перемикач *On*.

Далі для запису типу *CNAME* вкажемо назву сайта www.mysite1.ua , ім'я хоста *server0.mysite.ua*, натиснемо на кнопку *Add*. В результаті маємо отримати (рис.17.5).

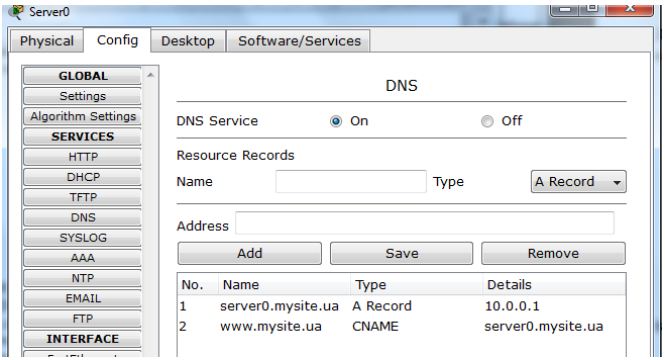

Рис. 17.5. Служба *DNS*

На вкладці *HTTP* змінимо початкову сторінку сайта:

```
<html>
<body>
<h1>Welcome to mysite.ua !! </h1>
<p>Server working: <font color="red"><b>OK!</b></font></p>
</body>
</html>
```

На Server1 налаштуємо *DHCP* (рис.17.6):

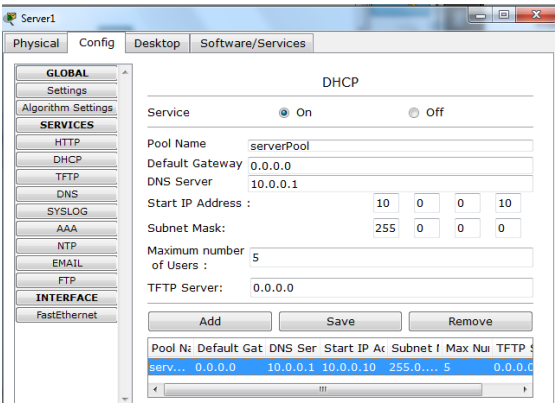

Рис. 17.6. Налаштування *DHCP* сервера

У командному рядку для *PC0* та *Laptop0* командою *ipconfig /release* очистимо старі параметри *IP*-адреси, а командою *ipconfig /renew* отримаємо нові параметри від *DHCP* сервера. Залишилося

перевірити роботу *HTTP* сервера. На *PC0* або *Laptop0* відкриємо в браузері сайт www.mysite.ua (рис.17.7):

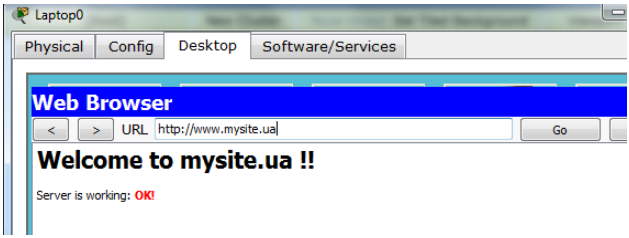

Рис. 17.7. Перевірка роботи служби *HTTP* на *Server0*

Також для перевірки правильності роботи прямої зони *DNS* сервера можна ввести команду *SERVER> nslookup*. Якщо все правильно налаштовано, то отримаєте відгук на запит із зазначенням доменного імені *DNS* сервера в мережі і його *IP*-адреси.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл.17.1. Побудувати мережу (див. рис.17.4).

Таблиця 17.1

Завдання

Номер варіанта	*IP*-адреса *Server* 0	*IP*-адреса *Server* 1	Назва сайту
1	10.10.0.1	10.10.0.2	*www.compnet10.ua*
2	20.20.0.1	20.20.0.2	*www.compnet20.ua*
3	30.30.0.1	30.30.0.2	*www.compnet30.ua*
4	40.40.0.1	40.40.0.2	*www.compnet40.ua*
5	50.50.0.1	50.50.0.2	*www.compnet50.ua*
6	60.60.0.1	60.60.0.2	*www.compnet60.ua*
7	70.70.0.1	70.70.0.2	*www.compnet70.ua*
8	80.80.0.1	80.80.0.2	*www.compnet80.ua*
9	90.90.0.1	90.90.0.2	*www.compnet90.ua*
10	100.100.0.1	100.100.0.2	*www.compnet100.ua*

4. Налаштувати *DHCP* на *Server1*, *Web* та *DNS* на *Server0*. Перевірити працездатність мережі. Відкрити сайт із *PC0* та *Laptop0*. На сторінці сайта вказати своє прізвище, ім'я, номер групи.

5. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Що таке *DNS*?
2. Для чого використовується *DNS*?
3. Як відбувається зв'язок в мережі, в якій існує сервер *DNS*?
4. З чого складається таблиця *DNS*?
5. Які дії виконує локальний *DNS* сервер, якщо не може знайти відповідність у своїй таблиці?
6. Як налаштувати *DNS* сервер?
7. Що таке *HTTP* (*Web*) сервер?
8. Які налаштування необхідно виконати для *HTTP* сервера?
9. Як додати або видалити сторінку із сайта на *HTTP* сервері?

Лабораторна робота 18
НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ МЕРЕЖНОГО СЕРВІСУ ЕЛЕКТРОННОЇ ПОШТИ В CISCO PACKET TRACER

Мета: ознайомитись з принципами організації взаємодії прикладних програм за допомогою протоколів електронної пошти *SMTP* та *POP3* в режимі симуляції *Cisco Packet Tracer*.

Основні теоретичні відомості

Основним компонентом системи передавання пошти є *MTA* (*Mail Transfer Agent*). Зазвичай користувачі безпосередньо не працюють з *MTA*, а користуються *MUA* (*Mail User Agent*) – клієнтом електронної пошти. Для передавання повідомлень через *TCP*-з'єднання більшість поштових агентів використовують протокол *SMTP* (*Simple Mail Transfer Protocol*). Він прийнятий як стандартний метод передавання електронної пошти в мережі Internet. Діючий стандарт протоколу описаний в *RFC* 2821. Транспортний протокол *SMTP* використовує *TCP*, з'єднання встановлюється через порт з номером 25. Для обслуговування цього з'єднання викорис-

товується спеціальна програма – поштовий сервер. Для формування повідомлення і встановлення з'єднання використовується поштова програма користувача. Після встановлення з'єднання обмін інформацією відбувається через команди. Для користувача ці команди не доступні, якщо для роботи він користується клієнтом електронної пошти.

Головною метою протоколу *SMTP* є надійна та ефективна доставка електронних поштових повідомлень. Для реалізації протоколу потрібен тільки надійний канал зв'язку. Середовищем для *SMTP* може бути окрема локальна мережа, мережна система або *Internet*.

Передавання зазвичай відбувається безпосередньо з хоста відправника на хост отримувача, коли обидва хоста використовують один транспортний сервіс. Якщо хости використовують різні сервіси, то передавання відбувається з використанням одного або декількох проміжних серверів *SMTP*.

Протокол *SMTP* використовує наступну модель комунікації: у відповідь на запит користувача поштова програма-відправник повідомлення встановлює двосторонній зв'язок з програмою-приймачем (поштовим сервером). Одержувачем може бути кінцевий або проміжний адресат. Якщо необхідно, поштовий сервер може з'єднатися з іншим сервером і передати повідомлення далі.

Для того щоб отримати повідомлення зі своєї поштової скриньки, поштова програма користувача з'єднується із сервером вже не за протоколом *SMTP*, а за спеціальним поштовим протоколом отримання повідомлень. Такий протокол дозволяє працювати з поштовою скринькою: забирати повідомлення, видаляти повідомлення, сортувати їх і виконувати інші операції. Найпопулярнішим в даний час протоколом такого роду є протокол *Post Office Protocol* v.3 (*POP3*).

Багато концепції, принципи і поняття протоколу *POP3* виглядають і функціонують подібно *SMTP*: взаємодія відбувається за допомогою команд. Сервер *POP3* знаходиться між агентом користувача і поштовими скриньками. Він передбачає з'єднання з поштовим сервером на основі транспортного протоколу *TCP* через порт 110. Специфікація *POP3* визначена в документі *RFC* 1939.

Конструкція протоколу *POP3* забезпечує можливість користувачу звернутися до свого поштового сервера і вилучити пошту, що

накопичилася для нього. Користувач може отримати доступ до *POP3*-сервера з будь-якої точки *Internet*. При цьому він повинен запустити спеціальний поштовий агент, що працює за протоколом *POP3*, і налаштувати його для роботи зі своїм поштовим сервером. Повідомлення доставляються клієнтові за протоколом *POP3*, а надсилаються за допомогою *SMTP*. Тобто на комп'ютері користувача існують два окремих агенти-інтерфейсу до поштової системи – доставки (*POP3*) і відправки (*SMTP*).

Побудуємо мережу, зображену на рис. 18.1, налаштуємо *IP*-адреси. Як сервери електронної пошти виступають сервери 172.162.0.20 та 172.16.0.40. Спочатку налаштуємо *DNS* на сервері 172.16.0.20 – вибираємо вкладку *Config*, Services, *DNS*. Внесемо дані про новий запис (A *Record*): *Name* – server.ua, *Address* – 172.16.0.20, натискаємо *Add*. Потім додамо ще один запис про поштовий сервер: *Name – mail.ua, Address* - 172.16.0.40.

Тепер сконфігуруємо поштовий сервер 172.16.0.20 з підтримкою *SMTP* та *POP3*. Виберемо вкладку *Config*, *Services -> EMAIL*. Включаємо протоколи *SMTP* та *POP3*, вводимо *Domain Name – server*.ua. Створюємо обліковий запис для одного користувача *user1*, вводимо логін та пароль, заносимо запис в службу за допомогою кнопки «+».

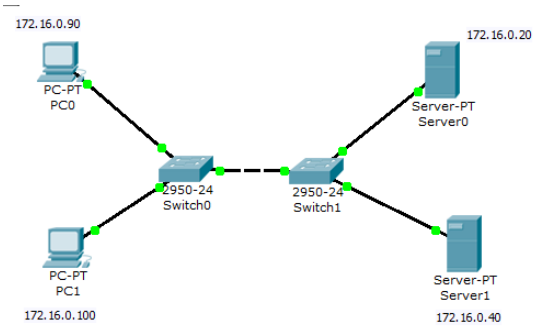

Рис. 18.1. Схема мережі

На сервері 172.16.0.40 також необхідно налаштувати поштовий сервер з підтримкою *SMTP* та *POP3*, як *DNS* для нього виступає сервер 172.16.0.20 (рис.18.2). Не забуваємо прописати *DNS* в налаштуваннях на *PC0* та *PC1*.

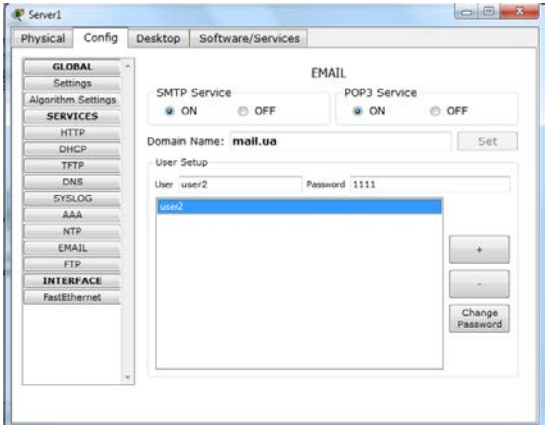

Рис. 18.2. Конфігурація *SMTP* та *POP3*-сервера

Тепер налаштуємо поштові служби на персональних комп'ютерах. На *PC0* переходимо на вкладку *Desktop*, вибираємо *E-mail*. У вікні, що з'явилося, вводимо налаштування поштового сервісу. Не забуваємо після зроблених налаштувань натиснути на кнопку *Save*. Аналогічні налаштування робимо і для *PC1* (рис.18.3).

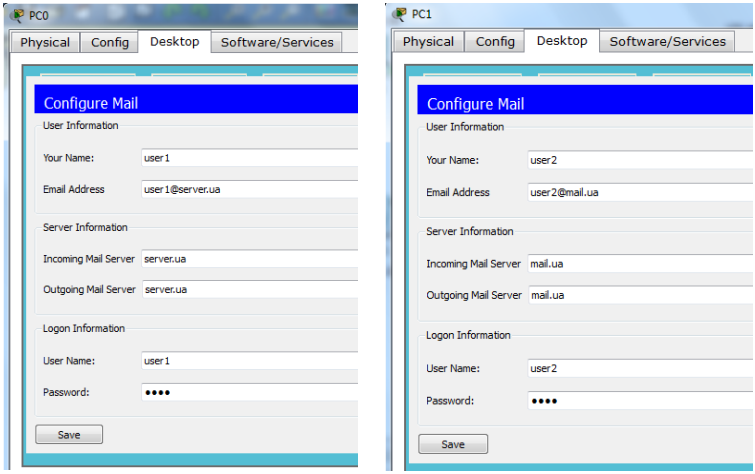

Рис. 18.3. Налаштування клієнтів електронної пошти

Надішлемо електронного листа з *PC0* на *PC1*. Перейдемо в режим моделювання, залишимо для відображення пакети *SMTP* та *POP3*. Відкриємо на *PC* вкладку *Desktop, E Mail*, для створення

листа натиснемо на *Compose*. В полі адресата *To* впишемо user2@mail.ua, а в полі теми листа *Subject – Hello*, текст листа довільний. Натиснемо на кнопку *Send*. Бачимо, що на *PC0* сформувався пакет. Натискаючи на кнопку *Capture*/*Forward* можемо спостерігати за переміщенням пакета спочатку на комутатори, потім на *Server0*, який звертається до служби *DNS* за *IP*-адресою заданого сервера. Потім пакет проходить через *Switch1* на *Server1*, де формується *SMTP*-відповідь для *Server0*. Після цього пакет залишається на сервері *mail.ua*.

Адресат (*PC1*) ще не отримав надісланого листа, оскільки сервер ще не звернувся до протоколу *POP3*. Для отримання листа необхідно на *PC1* вибрати у вкладці *Desktop* програму *E Mail* та натиснути на кнопку Receive, щоб прочитати лист. На *PC1* формується пакет протоколу *POP3*, натискаємо на кнопку *Capture*/*Forward* та прослідкуємо за маршрутом пакета через комутатори на *Server1*, а далі повертаємося на *PC1*. У вікні з'явилося повідомлення, натискаємо щоб прочитати його вміст (рис.18.4). В режимі моделювання можна переглянути вміст пакетів, що надсилаються (*PDU Information, Inbound PDU Details*).

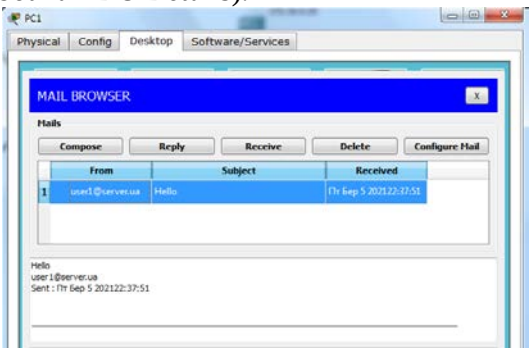

Рис. 18.4 Форма для перегляду вхідних листів

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл.18.1 та побудувати мережу (див. рис.18.1). Налаштувати *DNS*, *SMTP* та *POP3* відповідно до варіанта.

4. Відправити електронного листа від користувача на *PC0* до користувача на *PC1*, та надіслати листа у відповідь. Перевірити маршрути проходження пакетів в режимі моделювання.

5. Оформити звіт за результатами виконаної роботи.

Таблиця 18.1

Завдання

Номер варіанта	*PC0*	*PC1*	*Server0*	*Server1*
1	10.10.0.1	10.10.0.2	10.10.0.3, *mail10.ua*	10.10.0.4, *mail11.ua*
2	20.20.0.1	20.20.0.2	20.20.0.3, *mail20.ua*	20.20.0.4, *mail21.ua*
3	30.30.0.1	30.30.0.2	30.30.0.3, *mail30.ua*	30.30.0.4, *mail31.ua*
4	40.40.0.1	40.40.0.2	40.40.0.3, *mail40.ua*	40.40.0.4, *mail41.ua*
5	50.50.0.1	50.50.0.2	50.50.0.3, *mail50.ua*	50.50.0.4, *mail51.ua*
6	60.60.0.1	60.60.0.2	60.60.0.3, *mail60.ua*	60.60.0.4, *mail61.ua*
7	70.70.0.1	70.70.0.2	70.70.0.3, *mail70.ua*	70.70.0.4, *mail71.ua*
8	80.80.0.1	80.80.0.2	80.80.0.3, *mail80.ua*	80.80.0.4, *mail81.ua*
9	90.90.0.1	90.90.0.2	90.90.0.3, *mail90.ua*	90.90.0.4, *mail91.ua*
10	99.99.0.1	99.99.0.2	99.99.0.3, *mail98.ua*	99.99.0.4, *mail99.ua*

Запитання та завдання для самоперевірки

1. Що таке MTA?
2. Поясніть призначення протоколів *SMTP* та *POP3*?
3. Яка головна мета протоколу *SMTP*?
4. Яку модель комунікації використовує протокол *SMTP*?
5. Поясніть принцип роботи протоколу *POP3*.
6. Які налаштування необхідно виконати для налаштування *SMTP* та *POP3* на сервері?
7. Які налаштування необхідно виконати для налаштування *SMTP* та *POP3* на клієнті?
8. Поясніть шлях електронного листа від відправника до отримувача.
9. Як відслідкувати надсилання електронного листа в режимі моделювання?
10. З якою метою налаштовується *DNS* для реалізації *SMTP* та *POP3*?

Лабораторна робота 19
НАЛАШТУВАННЯ ПРОТОКОЛУ FTP В CISCO PACKET TRACER

Мета: аналіз принципів функціонування протоколів передавання файлів та отримання практичних навичок конфігурації протоколу *FTP* в *Cisco Packet Tracer*.

Основні теоретичні відомості

Стек протоколів *TCP*/*IP* містить три протоколи для передавання файлів: *FTP* (*File Transfer Protocol*), *TFTP* (*Trivial File Transfer Protocol*), *NFS* (*Network File System*). Протокол *FTP* є найбільш поширеним та затребуваним для передавання файлів мережею. *FTP* використовує клієнт-серверну архітектуру, в якій клієнт та сервер взаємодіють за схемою запит-відповідь.

Коли сервер отримує запит на файл, він відкриває *TCP*-з'єднання для клієнта і здійснює передавання. За допомогою *FTP*, працюючи на комп'ютері в одному населеному пункті можна підключитися до комп'ютера, розташованого в іншому пункті, і завантажити кілька файлів. При цьому необхідно знати ім'я облікового запису та пароль для віддаленого хоста. Користувачі Інтернету нерідко за допомогою *FTP* скачують різні файли (наприклад, мережні драйвери або поновлення системи). *FTP* призначений для передавання файлів цілком, що робить його зручним засобом для пересилання файлів великого розміру через глобальну мережу, він не дозволяє передати частину файла або деякі записи всередині файла. Оскільки дані вміщені в пакети *TCP*, комунікації з використанням *FTP* є надійними і забезпечуються механізмом служб із встановленням з'єднання. У *FTP*- комунікаціях виконується передавання одного потоку даних, в кінці якого є ознака кінця файла (*EOF*).

TFTP – це файловий протокол стека *TCP*/*IP*, призначений для передавання з деякого сервера файлів, що забезпечують завантаження бездискової робочої станції. Протокол *TFTP* не встановлює з'єднань і орієнтований на пересилання невеликих файлів в тих випадках, коли поява комунікаційних помилок не є критичним, і немає строгих вимог до безпеки.

NFS – протокол мережного доступу до файлових систем для операційних систем *UNIX*. *NFS* для обміну інформацією використовує виклики віддалених процедур (*RPC, Remote Procedure Calls*). Основна ідея полягає в тому, щоб дозволити групі користувачів поділяти використання загальної файлової системи.

FTP одночасно використовує декілька *TCP*-з'єднань – перше для керування процесом, друге (та інші) – безпосередньо для передавання даних. Режим передавання даних *FTP* може бути активним та пасивним, залежно від того, яка сторона (клієнт або сервер) є ініціатором встановлення з'єднання. В активному режимі керуюче з'єднання зініціюється клієнтом, а з'єднання передавання даних – сервером. В пасивному режимі обоє з'єднань ініціюються клієнтом.

Для взаємодії між клієнтом та сервером в протоколі *FTP* передбачено ряд спеціальних команд, які поділені на групи: команди керування доступом до системи (*user*, *pass*, *cwd*,*quit*), команди керування потоком даних (*port*, *type*, *stru*, *mode*) та команди *FTP*-сервісу (*stor*, *rnfr*, *rnto*, *abor*, *dele*).

Відповіді сервера складаються з трьох цифр та необов'язкових повідомлень, що можуть слідувати за цифрами, наприклад *1yz*, *2yz*, *x0z*, *x1z*, *x5z*.

Розглянемо налаштування *FTP* на прикладі мережі на рис.19.1. Спочатку налаштуємо *IP*-адреси та маски. На *FTP*-сервері відкриємо вкладку *Services*, виберемо *FTP*. Перевіримо, щоб служба була включена (перемикач «*On*»). В цьому ж вікні бачимо, що попередньо заданий логін (*cisco*) та пароль (*cisco*) для користувача, будемо використовувати цей обліковий запис.

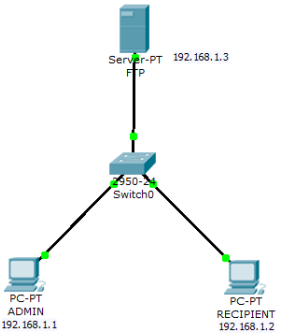

Рис. 19.1. Схема мережі

Відкриємо текстовий редактор на комп'ютері *ADMIN*, створимо файл, внесемо туди текст і збережемо під назвою *mes* (рис.19.2).

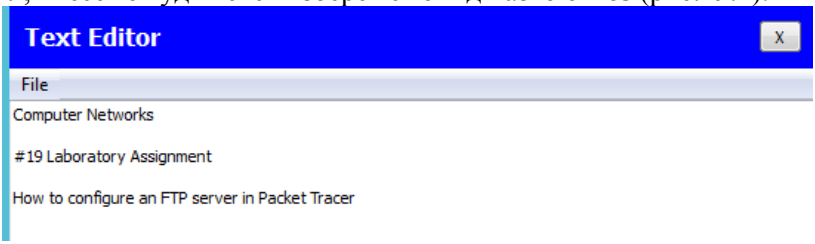

Рис. 19.2. Створення текстового файлу

У командному вікні за допомогою команди *put* виконаємо завантаження файла на *FTP*-сервер:

PC>ftp 192.168.1.3
Username:cisco
Password: // (пароль не відображається)
ftp>put mes.txt
Перевірка вмісту сервера:
ftp>dir.

У списку файлів, що стало доступним для відображення, переконайтеся в наявності файла mes.txt. тепер відкриємо командне вікно на комп'ютері *RECIPIENT*. Виконаємо завантаження файлу з *FTP*-сервера (рис.19.3):

PC>ftp 192.168.1.3
Username:cisco
Password: (пароль не відображається)
ftp>get mes.txt
Перевірка вмісту сервера:
ftp>dir

Файл *mes.txt* не видаляється із сервера після завантаження, а тому на комп'ютері *RECIPIENT* має з'явитися лише копія файла. Якщо завантаження пройшло успішно, то файл має відкритися на комп'ютері *RECIPIENT*. Зайдемо в текстовий редактор і відкриємо файл (рис.19.3).

File -> Open->mes.txt. Перевіримо, що текст на екрані відповідає тексту відправленого файла. У випадку повної відповідності, налаштування протоколу передавання даних *FTP* можна вважати коректним.

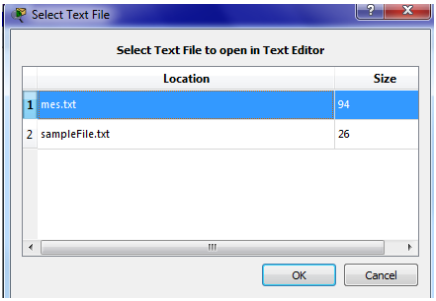

Рис. 19.3. Перевірка коректності налаштування протоколу *FTP*

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл.19.1 та побудувати мережу (див. рис.19.1). Налаштувати *FTP*-сервер (192.168.1.15).

Таблиця 19.1

Завдання

Номер варіанта	*PC0*	*PC1*	Назва файлів
1	192.168.1.1	192.168.1.10	*text1, text2*
2	192.168.1.2	192.168.1.20	*tester1, tester2*
3	192.168.1.3	192.168.1.30	*toseller1, toseller2*
4	192.168.1.4	192.168.1.40	*checking1, checking2*
5	192.168.1.5	192.168.1.50	*tfile1, tfile2*
6	192.168.1.6	192.168.1.60	*ftptest1, ftptest2*
7	192.168.1.7	192.168.1.70	*msg1, msg2*
8	192.168.1.8	192.168.1.80	*data1,data2*
9	192.168.1.9	192.168.1.90	*info1, info2*
10	192.168.1.99	192.168.1.109	*check1, check2*

4. Перевірити, чи активована служба *FTP* на сервері. Додати новий обліковий запис на сервері, встановивши логін (прізвище студента) та пароль.

5. Створити два текстові файли на комп'ютері *ADMIN*, внести в них текст та зберегти.

6. За допомогою команд *CLI* завантажити створені файли на FTP-сервер, переглянути вміст сервера.

7. На комп'ютері *RECIPIENT* завантажити із сервера створені файли, перевірити вміст завантажених файлів.

8. Видалити завантажені файли із *FTP*-сервера.

9. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Які ви знаєте протоколи передавання файлів?
2. Назвіть основні особливості *FTP*-протоколу.
3. Яку архітектуру використовує *FTP*? Поясність її суть.
4. Які особливості використання *TFTP* протоколу?
5. Яка відмінність між *FTP* та *TFTP*?
6. Поясність призначення протоколу *NFS*.
7. Яка основна ідея використання *NFS*?
8. Поясніть суть підходу «*stateless*» для *NFS*.
9. Які ви знаєте типи з'єднань протоколу *FTP*?
10. Охарактеризуйте режими передавання даних *FTP*.
11. Які групи команд використовуються в *FTP*?
12. Назвіть основні команди *FTP* та наведіть приклади їх використання.
13. Що таке коди відповідей *FTP*? Наведіть приклади.
14. Порівняйте вивчені протоколи.

Лабораторна робота 20
НАЛАШТУВАННЯ СТАТИЧНОГО NAT

Мета: ознайомлення з технологією трансляції мережних адрес *NAT*, налаштування статичного *NAT* в *Cisco Packet Tracer*.

Основні теоретичні відомості

NAT (*Network Address Translation*) – трансляція мережних адрес, технологія, яка дозволяє перетворювати (змінювати) *IP*-адреси і

порти в мережних пакетах. *NAT* використовується найчастіше для здійснення доступу пристроїв з локальної мережі підприємства в Інтернет, або навпаки для доступу з Інтернет на який-небудь ресурс всередині мережі. Локальна мережа підприємства будується на приватних *IP*-адресах:

10.0.0.0 - 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))

172.16.0.0 - 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))

192.168.0.0 - 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Ці адреси не маршрутизуються в Інтернеті, і провайдери повинні відкидати пакети з такими *IP*-адресами відправників або одержувачів. Для перетворення приватних адрес в глобальні (маршрутизовані в Інтернеті) застосовують *NAT*.

NAT – технологія трансляції мережних адрес, тобто підміни адрес (або портів) у заголовку *IP*-пакета. Іншими словами, пакет, проходячи через маршрутизатор, може поміняти свою адресу джерела і/або призначення.

Подібний механізм служить для забезпечення доступу з локальної мережі, де використовуються приватні *IP*-адреси, в Internet, де використовуються глобальні *IP*-адреси.

Існує три види трансляції *Static NAT, Dynamic NAT, Overloading* (*PAT*). В даній лабораторній роботі розглянемо *Static NAT*. *Static NAT* (статичний *NAT*) здійснює перетворення *IP*-адреси один до одного, тобто порівнюється одна адреса з внутрішньої мережі з однією адресою із зовнішньої мережі. Тобто під час проходження через маршрутизатор, адреса(и) змінюється на чітко задану адресу, один-до-одного. Наприклад, 10.1.1.5 завжди замінюється на 11.1.1.5 і назад. Запис про таку трансляцію зберігається необмежено довго, поки є відповідний рядок в конфігурації маршрутизатора.

Розглянемо налаштування статичного *NAT* на прикладі мережі (рис.20.1). Пропишемо задані *IP*-адреси. Як бачимо з рис.20.1, є зовнішня адреса 20.20.20.20 і внутрішня мережа 10.10.10.0. Якщо відправити пакет від *PC0* на *Server0* та в режимі моделювання переглянути структуру пакета, побачимо, що адреса відправника 10.10.10.1 не змінюється. Тепер налаштуємо *NAT*. На маршрутизатор додаємо *access*-list, дозволяємо все (*any*):

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#access-list 1 permit any
Router(config)#ip nat inside source list 1 interface fa 0/1 overload

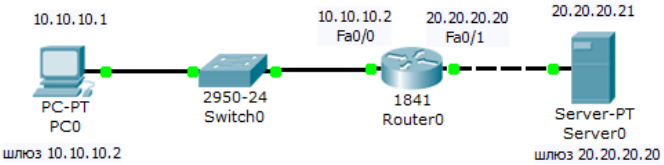

Рис. 20.1. Схема мережі

Тепер налаштуємо трансляцію на інтерфейсах (на внутрішньому *inside*, на зовнішньому - *outside*), тобто, для *R0* вказуємо внутрішній і зовнішній порти:

Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#ex
Router(config)#int fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#ex

Далі налаштовуємо адресу, вказуємо, що саме вхідні в цей інтерфейс повідомлення будуть транслюватися, вмикаємо інтерфейс, вказуємо, що саме вихідні з цього інтерфейсу повідомлення будуть транслюватися, задаємо статичну трансляцію адреси 10.10.10.1 в адресу 20.20.20.22:

Router#en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip addr 10.10.10.2 255.0.0.0
Router(config-if)#ip nat inside
Router(config-if)#no sh
Router(config-if)#int fa0/1
Router(config-if)#ip addr 20.20.20.20 255.0.0.0
Router(config-if)#ip nat outside
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#ip nat inside source static 10.10.10.1 20.20.20.22
Router(config)#

Виходимо з режиму глобального конфігурування і записуємо налаштування маршрутизатора в пам'ять:

Router(config)#end

Router#wr mem

В режимі моделювання відправимо пакет від *PC0* на *Server0*. Тепер бачимо, що на маршрутизаторі відбувається заміна *IP*-адрес (рис.20.2):

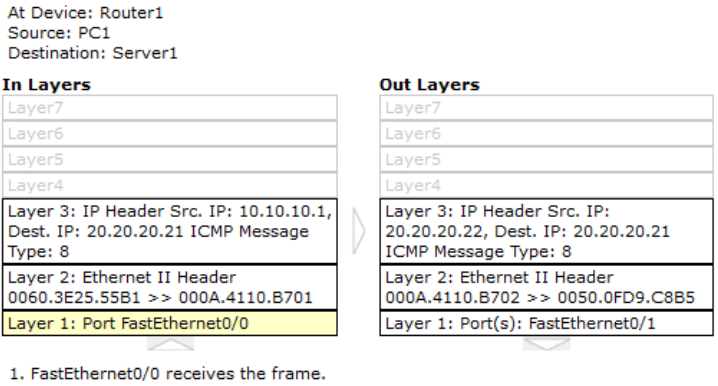

Рис. 20.2. Транслювання адреси під час проходження повідомлення від *PC0* до сервера

Для перегляду стану таблиці *NAT*, одночасно з ping використовуйте команду sh ip nat translations або за допомогою інструменту *Inspect* на панелі Common Tools Bar відкрийте на маршрутизаторі *Nat Table* під час виконання команди ping. Іншою корисною командою є *show ip nat statistics*, що відображає інформацію про загальну кількість активних переходів, параметри конфігурації *NAT*. Щоб впевнитися, що трансляція *NAT* працює, краще очистити статистику попередніх замін, використовуючи команду *clear ip nat statistics* перед тестуванням.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл.20.1 та побудувати мережу (рис.20.3). Як *Default Gateway* для *PC2* встановити *IP*-адресу інтерфейсу Fa 0/0 маршрутизатора *Router2*. Налаштувати *NAT*.
4. Переглянути інформацію про загальну кількість переходів та параметри конфігурації *NAT*. Записати вміст таблиці *NAT*.

5. Оформити звіт за результатами виконаної роботи.

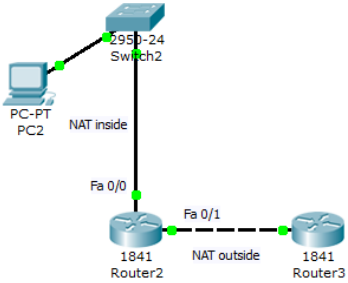

Рис. 20.3. Схема мережі до завдання

Таблиця 20.1

Завдання

Номер варіанта	*PC2*	*Router2 Fa 0/0*	*Router2 Fa 0/1*	*Router3 Fa 0/1*	*зовнішня адреса NAT*
1	10.10.10.2	10.10.10.1	200.20.20.1	200.20.20.2	200.20.20.10
2	10.10.10.4	10.10.10.2	200.20.20.3	200.20.20.4	200.20.20.30
3	10.10.10.6	10.10.10.3	200.20.20.5	200.20.20.6	200.20.20.50
4	10.10.10.8	10.10.10.4	200.20.20.7	200.20.20.8	200.20.20.70
5	10.10.10.10	10.10.10.5	200.20.20.9	200.20.20.10	200.20.20.90
6	10.10.10.12	10.10.10.6	200.20.20.11	200.20.20.12	200.20.20.15
7	10.10.10.14	10.10.10.7	200.20.20.13	200.20.20.14	200.20.20.25
8	10.10.10.16	10.10.10.8	200.20.20.15	200.20.20.16	200.20.20.35
9	10.10.10.18	10.10.10.9	200.20.20.17	200.20.20.18	200.20.20.45
10	10.10.10.20	10.10.1010	200.20.20.19	200.20.20.20	200.20.20.55

Запитання та завдання для самоперевірки

1. Що таке *NAT*?
2. Для чого використовується *NAT*?
3. Опишіть технологію трансляції мережних адрес.
4. Які види трансляції адрес ви знаєте?
5. Які команди використовуються для налаштування статичного *NAT*?
6. Як перевірити стан таблиці *NAT*?
7. Як відобразити інформацію про загальну кількість активних переходів, параметри конфігурації *NAT*?
8. Як очистити статистику попередніх замін *NAT*?

Лабораторна робота 21
НАЛАШТУВАННЯ ДИНАМІЧНОГО NAT

Мета: налаштування динамічної трансляції адрес в *Cisco Packet Tracer*.

Основні теоретичні відомості

Dynamic NAT (динамічний *NAT*) перетворює внутрішні адреси в одну з групи зовнішніх адрес. Тобто, перед використанням динамічної трансляції, потрібно задати список зовнішніх адрес. В цьому випадку під час проходження через маршрутизатор, нова адреса вибирається динамічно з деякого діапазону адрес, що називають пулом (*pool*). Запис про трансляцію зберігається деякий час, щоб відповідні пакети могли бути доставлені адресату. Якщо протягом деякого часу трафік за цією трансляцією відсутній, трансляція видаляється і адреса повертається в пул. Якщо потрібно створити трансляцію, а вільних адрес в пулі немає, то пакет відкидається. Тобто кількість внутрішніх адрес має бути ненабагато більшою за кількість адрес в пулі, інакше існує висока ймовірність проблем з виходом у зовнішню мережу.

Розглянемо налаштування динамічного *NAT* на прикладі мережі (рис.21.1).

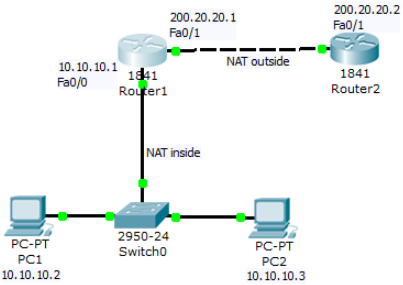

Рис. 21.1. Схема мережі

Налаштуємо на маршрутизаторі *R1* список доступу, відповідний адресам внутрішньої мережі (0.0.0.225 – зворотна (інверсна) маска для адреси 10.10.10.0):

R1 (config)# access-list 1 permit 10.10.10.0 0.0.0.255

Далі вкажемо пул зовнішніх адрес та налаштуємо трансляції:

R1 (config)# ip nat pool white-address 200.20.20.3 200.20.20.30 netmask 255.255.255.0

R1 (config)# ip nat inside source list 1 pool white-address

Потім налаштуємо внутрішній та зовнішній інтерфейси, запишемо у пам’ять:

R1 (config)# int fa 0/0
R1 (config-if)# ip nat inside
R1 (config-if)#ex
R1 (config)# int fa 0/1
R1 (config-if)# ip nat outside
R1 (config-if)#ex
Router(config)#ex
Router#wr

Для перевірки налаштувань відправимо в режимі моделювання пакети з *PC1* на *R2* та одночасно пропишемо команду на маршрутизаторі *show ip nat translations* (рис. 21.2).

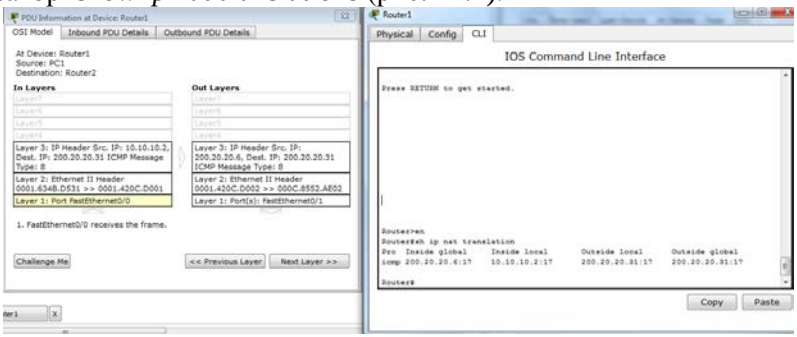

Рис. 21.2. Трасляція адрес динамічного *NAT*

Командою *show ip nat statistics* можна подивитися статистику по *NAT* перетворенням.

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл .21.1, побудувати мережу (рис. 21.3), налаштувати *NAT*, *DNS* та *HTTP*-сервери. В таблиці задано пул адрес мережі, *IP*-адреси вузлів вибрати довільно із заданого пулу.

4. Для перевірки зроблених налаштувань відкрити з будь-якого *PC* сайт. На сторінці має бути інформація про прізвище, ім'я студента, номер групи, номер та назва лабораторної роботи.

5. Переглянути інформацію про загальну кількість переходів та параметри конфігурації *NAT*. Записати вміст таблиці *NAT*.

6. Оформити звіт за результатами виконаної роботи.

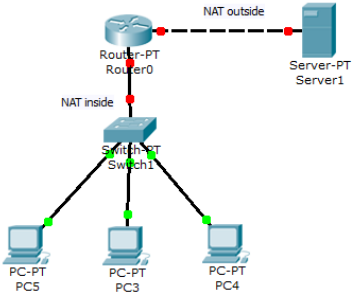

Рис. 21.3. Схема мережі до завдання

Таблиця 21.1

Завдання

Номер варіанта	Внутрішня мережа	Зовнішня мережа	Сайт
1	10.10.10.0-10.10.10.10	200.10.10.0-200.10.10.10	*CN1.com*
2	10.10.10.11-10.10.10.20	200.10.10.11-200.10.10.20	*CN2.com*
3	10.10.10.21-10.10.10.30	200.10.10.21-200.10.10.30	*CN3.com*
4	10.10.10.31-10.10.10.40	200.10.10.31-200.10.10.40	*CN4.com*
5	10.10.10.41-10.10.10.50	200.10.10.41-200.10.10.50	*CN5.com*
6	10.10.10.51-10.10.10.60	200.10.10.51-200.10.10.60	*CN6.com*
7	10.10.10.61-10.10.10.70	200.10.10.61-200.10.10.70	*CN7.com*
8	10.10.10.71-10.10.10.80	200.10.10.71-200.10.10.80	*CN8.com*
9	10.10.10.81-10.10.10.90	200.10.10.81-200.10.10.90	*CN9.com*
10	10.10.10.91-10.10.10.100	200.10.10.91-200.10.10.100	*CN10.com*

Запитання та завдання для самоперевірки

1. Що таке динамічний *NAT*?
2. Опишіть технологію динамічної трансляції мережних адрес.
3. Які команди використовуються для налаштування динамічного *NAT*?
4. Які відмінності між статичним та динамічним *NAT*?

Лабораторна робота 22
СТВОРЕННЯ СПИСКІВ ДОСТУПУ ACL

Мета: ознайомитися з принципами побудови списків доступу в *Cisco Packet Tracer*.

І. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

ACL (Access Control List) – це набір текстових виразів, які щось дозволяють, або щось забороняють. Зазвичай *ACL* дозволяє або забороняє *IP*-пакети, але крім усього іншого він може заглядати всередину *IP*-пакета, переглядати тип пакета, *TCP* і *UDP* порти. Також *ACL* існує для різних мережних протоколів (*IP*, *IPX*, *AppleTalk*). В основному застосування списків доступу розглядають з точки зору пакетної фільтрації. Розміщується *ACL* на вхідному напрямку і блокує надлишкові види трафіку.

Сам же *ACL* являє собою набір текстових виразів, у яких написано *permit* (дозволити) або *deny* (заборонити), і обробка ведеться строго в тому порядку в якому задані вирази. Відповідно коли пакет потрапляє на інтерфейс, він перевіряється на першу умову, якщо перша умова збігається з пакетом, подальша його обробка припиняється. Пакет або перейде далі, або знищиться.

ACL поділяються на два типи:

• стандартні (*Standard*): можуть перевіряти тільки адреси джерел;

• розширені (*Extended*): можуть перевіряти адреси джерел, а також адреси отримувачів, в разі IP ще тип протоколу і *TCP*/*UDP* порти.

Позначаються списки доступу або номерами, або символьними іменами, стандартні: від 1 до 99, розширені: від 100 до 199.

Для фільтрації адрес в *ACL* використовується *WildCard*-маска. Це зворотна маска. Вона вираховується так: беремо шаблонний вираз, віднімаємо від шаблону звичайну маску:

255.255.255.255 – 255.255.255.0= 0.0.0.255.

Розглянемо в даній роботі створення стандартних та розширених списків доступу. У стандартних *ACL* є можливість задати лише IP адресу джерела пакетів для їх заборони або дозволів. Побудуємо мережу, що складається з двох підмереж 192.168.0.0 та 10.0.0.0 (рис. 22.1). Налаштуємо *IP*-адреси. Надішлемо пакети від *PC0* та

PC1 на сервер і в зворотному напрямку. Якщо мережа налаштована правильно, всі пакети надходять успішно.

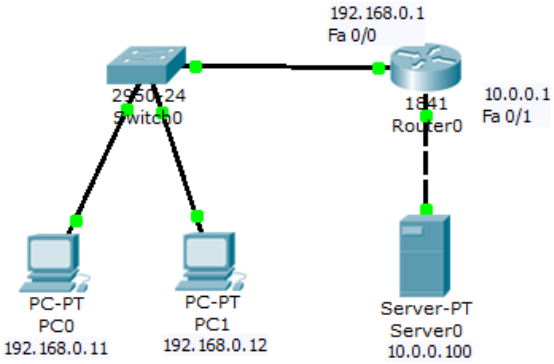

Рис. 22.1. Схема мережі

Дозволимо доступ на сервер для *PC1*, а для *PC0* – заборонимо. Правило заборони і дозволу доступу будемо складати з використанням стандартних списків доступу *ACL*. Поки не заданий список доступу на інтерфейсі – все дозволено (*permit*). Але варто створити список, як відразу діє механізм "Все, що не дозволено, то заборонено". Тому немає необхідності щось забороняти (*deny*) – вказуємо що дозволено, а "іншим – заборонити" встановлюється автоматично. Застосовується дане правило на інтерфейс залежно від напрямку (*PC1* розташований з боку порту *Fa0*/0), тобто список доступу (правило з номером 1) діятиме на інтерфейсі fa0/0 на вхідному (*in*) від *PC1* напрямку. На маршрутизаторі введемо відповідні команди:

Router>en
Router#conf t
Router(config)#access-list 1 permit host 192.168.0.12
Router(config)#int fa0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#ex

Вхідний трафік (*in*) – цей той, який приходить на інтерфейс ззовні. Вихідний трафік (*out*) – той, який відправляється з інтерфейсу зовні. Список доступу можна застосувати або на вхідний трафік, тоді небажані пакети не будуть навіть потрапляти на маршрутизатор і відповідно, далі в мережу, або на вихідний, тоді пакети над-

ходять на маршрутизатор, обробляються ним, доходять до цільового інтерфейсу і тільки на ньому обробляються. Як правило, списки застосовують на вхідний трафік (*in*).

Перевіримо зв'язок *PC0* та *PC1* із сервером (рис. 22.2).

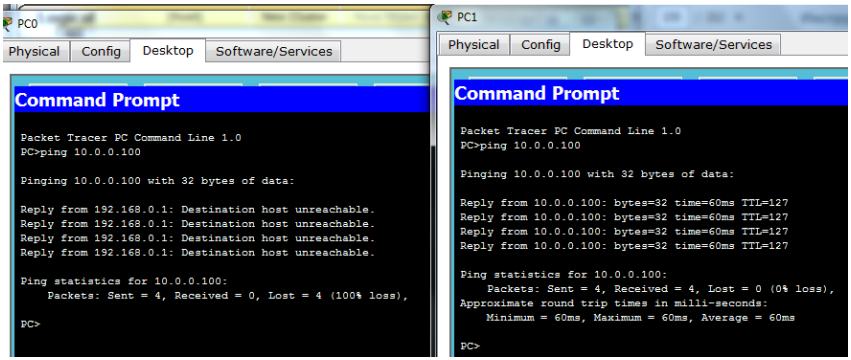

Рис. 22.2. Наявність зв’язку *PC0* та *PC1* із сервером

Щоб переглянути список *ACL* введемо на маршрутизаторі команду *sh access-lists*. Результатом її виконання має бути перелік дозволених *IP*-адрес, в нашому випадку результатом виконання є:

Standard IP access list 1
permit host 192.168.0.12 (8 match(es))

Якщо потрібно додати до існуючого списку *ACL* новий вузол, наприклад *PC2* з *IP*-адресою 192.168.0.15 як дозволений, то необхідно на маршрутизаторі ввести ще одну команду:

Router (config)#accesslist 1 permit host 192.168.0.15

Для відміни будь-якого правила повторюємо його з приставкою "*no*". Наприклад, якщо виконати команду *no ip access*-group *1 in*, то *ACL* буде відмінено.

На відміну від стандартних списків, для розширених в правилах доступу можна включати фільтрацію трафіку за протоколами і портами.

Для вказівки портів в правилі доступу вказуються такі позначення (табл. 22.1).

Таблиця 22.1

Позначення портів в *ACL*

Позначення	Дія
lt n	Усі номери портів, менші за *n*
gt n	Усі номери портів, більші за *n*
eq n	Порт *n*
neq n	Усі порти, за виключенням *n*
range n m	Усі порти від *n* до *m* включно

Розглянемо налаштування розширених списків *ACL* на прикладі мережі (рис. 22.3). Заборонимо доступ до *Server2* для *PC3* і дозволимо для *PC4*.

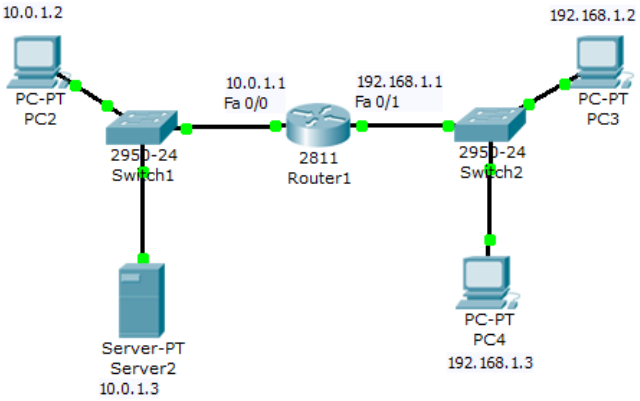

Рис. 22.3. Схема мережі

Налаштуємо на *Server2 FTP* з логіном та паролем *Cisco*. Переконаємося, що сервер працює і доступ до нього є.

Виконаємо команду *DIR* – читання директорії на *PC2* (рис.22.4):

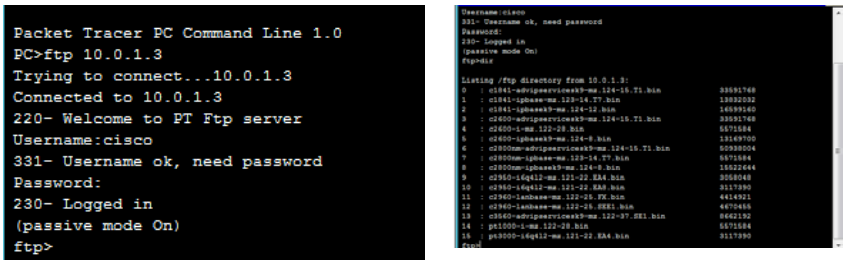

Рис. 22.4 *FTP*-сервер працює

Створимо список правил з номером 101, в якому вкажемо 2 дозволяючих і по 2 забороняючих правила для портів сервера 21 і 20 (ці порти служать для *FTP*- передавання команд і даних):

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 21
Router(config-ext-nacl)#permit tcp 192.168.1.2 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 20
Router(config-ext-nacl)#deny tcp 192.168.1.3 0.0.0.0 10.0.1.3 0.0.0.0 eq 21
```

Потім застосуємо список 101 на вхід (*in*) *Fa0*/1, оскільки трафік входить на цей порт маршрутизатора з боку мережі 192.168.1.0:

```
Router(config-ext-nacl)#int fa0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#ex
Router(config)#ex
Router#wr mem
```

Перевіримо зв'язок сервера з *PC4*, ввівши в командному рядку *PC>ftp* 10.0.1.3 та спробуємо переглянути директорії за допомогою команди *DIR*.

Якщо налаштування виконано правильно, *FTP*-сервер буде недоступний (рис.22.5):

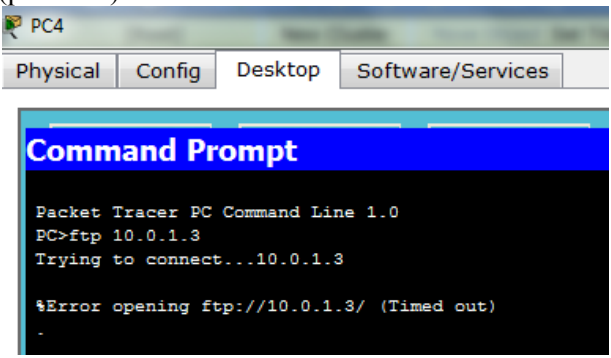

Рис. 22.5. *FTP*-сервер для *PC4* недоступний

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл. 22.2, побудувати мережу (рис. 22.6).

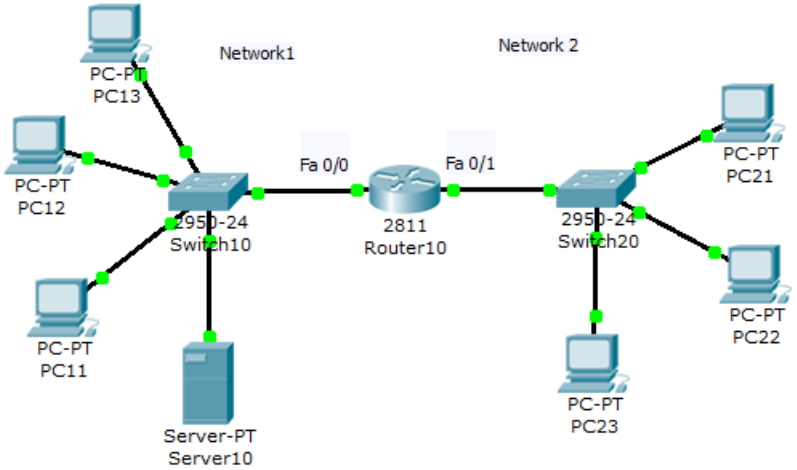

Рис. 22.6 Схема мережі до завдання

Таблиця 22.2

Завдання

Номер варіанта	*Network1*	*Network2*	Заборонено доступ на сервер
1	10.10.10.0-10.10.10.10	200.10.10.0-200.10.10.10	*PC11,PC33,PC22*
2	10.10.10.11-10.10.10.20	200.10.10.11-200.10.10.20	*PC12,PC21,PC23*
3	10.10.10.21-10.10.10.30	200.10.10.21-200.10.10.30	*PC11,PC12,PC22*
4	10.10.10.31-10.10.10.40	200.10.10.31-200.10.10.40	*PC12,PC33,PC22*
5	10.10.10.41-10.10.10.50	200.10.10.41-200.10.10.50	*PC13,PC13,PC22*
6	10.10.10.51-10.10.10.60	200.10.10.51-200.10.10.60	*PC13,PC21,PC22*
7	10.10.10.61-10.10.10.70	200.10.10.61-200.10.10.70	*PC12,PC22,PC23*
8	10.10.10.71-10.10.10.80	200.10.10.71-200.10.10.80	*PC12,PC21,PC22*
9	10.10.10.81-10.10.10.90	200.10.10.81-200.10.10.90	*PC11,PC33,PC21*
10	10.10.10.91-10.10.10.100	200.10.10.91-200.10.10.100	*PC13,PC33,PC22*

4. Налаштувати *IP*-адреси відповідно до варіанта, адреси вибрати довільно із заданого пулу.

5. Налаштувати *FTP*-сервер, записати на нього із кожного *PC* файл. Перевірити наявність файлів на сервері.

6. Налаштувати *ACL* список відповідно до варіанта. Перевірити список доступу за допомогою команди *sh access-lists*.

7. Завантажити на кожен *PC* файли з *FTP*-сервера, яких немає на цьому *PC*.

8. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Що таке списки доступу?
2. Де застосовуються списки доступу (*ACL*)?
3. На які типи поділяються *ACL*?
4. Поясніть поняття стандартних та розширених списків доступу.
5. Назвіть види списків доступу.
6. Що таке динамічний список доступу (*Dynamic* ACL)?
7. Що таке рефлексивний список доступу (*Reflexive ACL*)?
8. Коли застосовують обмеження за часом (*Time-based ACL*)?
9. Що таке *WildCard*-маска?
10. Які команди застосовують для налаштувань списку *ACL*?

Лабораторна робота 23
СТВОРЕННЯ ТА НАЛАШТУВАННЯ БЕЗДРОТОВОЇ МЕРЕЖІ В CISCO PACKET TRACER

Мета: ознайомитися із загальними принципами створення та налаштування бездротових мереж, аналізу та визначення параметрів бездротових мереж в *Cisco Packet Tracer*.

Основні теоретичні відомості

Як носій інформації бездротових мереж будемо розглядати радіохвилі НВЧ-діапазону, що підпорядковуються стандарту *IEEE* 802.11, відомому як *Wi-Fi*. *Wi-Fi* – це система короткої дії, що зазвичай покриває десятки метрів, яка використовує неліцензовані діапазони частот для забезпечення доступу до мережі. Зазвичай *Wi-Fi* використовується користувачами для доступу до їх власної локальної мережі, яка може бути і не підключена до Інтернету.

WEP (*Wired Equivalent Privacy*) – алгоритм для забезпечення безпеки мереж Wi-Fi. Використовується для забезпечення захисту переданих даних.

Для побудови бездротової мережі *Wi-Fi* використовують точки доступу *Wi-Fi* та адаптери *Wi-Fi*. Точка доступу (*Access Point, AP*) – це окремий мікрокомп'ютерний пристрій з приймально-передавальним радіотрактом. Вона виконує роль комутатора, забезпечуючи взаємодію та обмін інформацією між бездротовими адаптерами, а також зв'язок з провідним сегментом мережі. Такий зв'язок виконується через мережний інтерфейс (*Uplink Port*). Через цей же інтерфейс може здійснюватися й налаштування точки доступу.

Точка доступу може використовуватися як для підключення до неї клієнтів (базовий режим), так і для взаємодії з іншими точками доступу для побудови розподіленої мережі (*Wireless Distributed System, WDS*). Це режими бездротового мосту «точка–точка» і «точка–багато точок», бездротовий клієнт і повторювач.

Адаптер – це пристрій, який підключається через слот розширення *PCI, PCMCI, CompactFlash* або через порт *USB* 2.0. Він фактично виконує ту ж функцію, що й мережний адаптер (карта) у провідній мережі й слугує для підключення комп'ютера користувача до бездротової мережі. Варто зазначити, що усі сучасні ноутбуки, мобільні телефони, планшети мають вбудовані адаптери, які сумісні з багатьма сучасними стандартами.

Створення нової бездротової мережі починається безпосередньо з конфігурації точки доступу – бездротового маршрутизатора (роутера), підключення до неї комп'ютерів та іншого бездротового обладнання.

Класичний спосіб налаштування такий: спочатку проводиться підключення до точки доступу обладнання, а потім потрібно задати вручну ім'я бездротової мережі і ключ безпеки. В даній лабораторній роботі далі ми розглянемо різні варіанти бездротових мереж і способи їх налаштування в програмі *Cisco Packet Tracer*.

Ключ безпеки бездротової мережі – унікальний код (пароль), який закриває доступ до мережі. важливим є не стільки сам ключ, скільки тип шифрування. Вся інформація, яка протікає між комутатором і ПК, шифрується. І якщо було введено неправильний ключ, то пристрій просто не зможе розкодувати отриману інформацію.

Це зроблено для підвищення безпеки. Існує три типи шифрування *Wi-Fi* підключень: *WPA*, *WPA2*, *WEP*.

Розглянемо приклади налаштувань бездротових мереж.

Приклад 1. Спочатку налаштуємо бездротову мережу *WEP*. Побудуємо схему (рис.23.1).

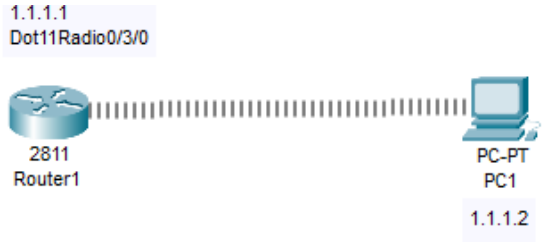

Рис. 23.1. Схема мережі до завдання

Додамо до маршрутизатора радіоточку доступу (рис.23.2).

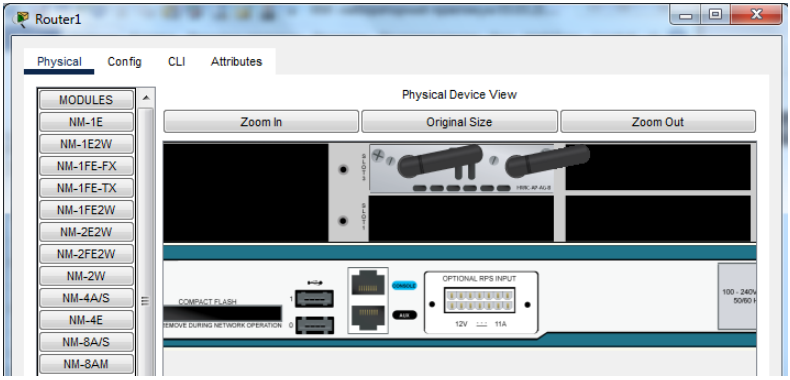

Рис. 23.2. Радіоточка доступу *HWIC-AP-AG-B*

Для цього перейдемо у вкладку *Physical*, вимкнемо кнопку живлення маршрутизатора, та перетягнемо із лівої області модулів радіоточку доступу *HWIC-AP-AG*-B.

Тепер перейдемо до налаштувань *PC*. На вкладці *Physical*, вимкнемо кнопку живлення, видалимо наявний модуль *PT-HOST-NM-1CFE* (необхідно перетягти модуль вліво на перелік наявних модулів), а на його місце ставимо модуль бездротовий адаптер *WMP300N* (рис.23.3).

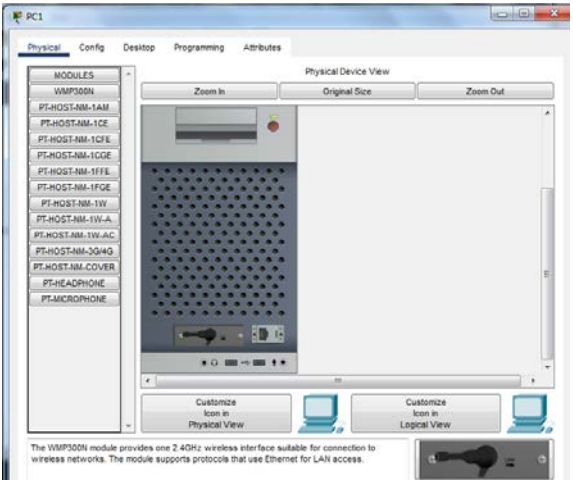

Рис. 23.3. Заміна модуля *PT-HOST-NM-1CFE* на *WMP300N*

Налаштуємо бездротовий адаптер на *PC1*. Перейдемо на вкладку *Config*, виберемо *Wireless*. В полі *SSID* введемо *Admin*, виберемо перемикач *WEP*, в поле *WEP Key* введемо пароль, наприклад 1234567890, а також налаштуємо статичну *IP*-адресу 192.168.10.2 та маску 255.255.255.0.

Налаштуємо точку доступу на маршрутизаторі:

Router>en
Router#conf t
Router(config)#dot11 ssid Admin
Router(config-ssid)#authentication open
Router(config-ssid)#guest-mode
Router(config-ssid)#exit
Router(config)#int dot11Radio 0/3/0
Router(config-if)#encryption mode wep mandatory
Router(config-if)#encryption key 1 size 40bit 1234567890
Router(config-if)#ssid Admin
Router(config-if)#ip address 1.1.1.1 255.0.0.0
Router(config-if)#no shutdown

Перевіримо результат – між маршрутизатором і *PC1* з'явився бездротовий зв'язок. Перевіримо командою ping з *PC1* на 1.1.1.1 – всі пакети отримано.

Типи шифрування мережі *WPA* і *WPA2* вимагають від абонентів введення унікального пароля. Без нього ви просто не зможете виконати підключення. Після перевірки введеного ключа всі дані, які передаються між учасниками мережі, шифруються. Сучасні маршрутизатори підтримують обидві технології. Але, *WPA2* все ж надає більш високий захист. Тому за можливості слід вибирати саме його.

Приклад 2. Розглянемо налаштування бездротової мережі із використанням *WPA* (рис. 23.4).

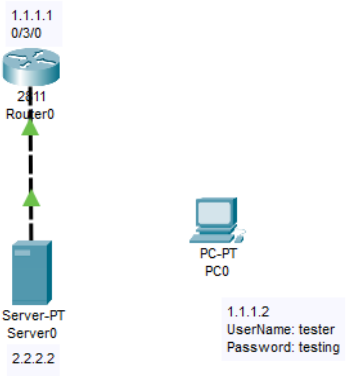

Рис. 23.4. Схема мережі для налаштування із використанням *WPA*

Маршрутизатор та *PC* не мають бездротового адаптера, тому як і в попередньому прикладі, замінимо модуль *PT-HOST-NM-1CFE* на *WMP300N* для *PC* та додамо модуль *HWIC-AP-AG-B* на маршрутизатор. Далі налаштуємо маршрутизатор:

Router>enable
Router#configure terminal
Router(config)#interface Dot11Radio0/3/0
Router(config-if)#
Router(config-if)#ex
Router(config)#dot11 ssid Adm
Router(config-ssid)#authentication open
Router(config-ssid)#authentication key-management wpa
Router(config-ssid)#wpa-psk ascii 0 12345678
Router(config-ssid)#guest-mode
Router(config-ssid)#ex
Router(config)#interface dot11radio0/3/0

Router(config-if)#ip address 1.1.1.1 255.0.0.0
Router(config-if)#ssid Adm
Router(config-if)#encryption mode ciphers aes-ccm
Router(config-if)#no shutdown

Далі налаштуємо *PC*. На вкладці *Config* виберемо *Wireless0*, встановимо *SSID – Adm*, *Autnentication – WPA-PSK*, *PKS Pass Phrase* – 12345678, *IP*-адресу 1.1.1.2, маску 255.0.0.0, *Default Gateway* 1.1.1.1. Як тільки на *PC* було зроблено налаштування, бездротовий зв'язок між *PC* та маршрутизатором встановлено (рис. 23.5). Відправимо пакет від *PC* на *Server* – результат *Successful*.

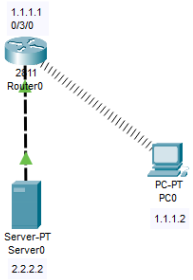

Рис. 23.5. Наявність з'єднання в мережі

Приклад 3. Бездротова мережа з точкою доступу. Побудуємо схему (рис. 23.6). Налаштуємо інтерфейси маршрутизатора, вкажемо відповідні IP-адреси та маски.

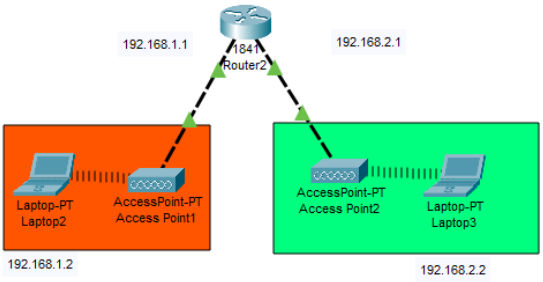

Рис. 23.6. Схема мережі

Для *Laptop* встановимо адаптери *PC300N*, налаштуємо відповідні *IP*-адреси та *Default Gateway*. Для *Wireless* інтерфейсів ноутбуків вкажемо відповідні *SSID – Office1* (для *Laptop2*) *Office2* (для

Laptop3), решту налаштувань бездротового інтерфейсу залишаємо без змін. Для обох точок доступу вказуємо відповідні *SSID* – *Office1* (для *AccessPoint1*) *Office2* (*AccessPoint2*). Необхідні налаштування для бездротової мережі з точкою доступу виконані. Перевіряємо зв'язок між *Laptop* (рис. 23.7):

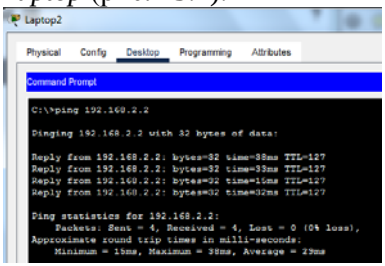

Рис. 23.7 Зв'язок між *Laptop2* та *Laptop3*

Приклад 4. Бездротовий зв'язок в *Packet Tracer* з бездротовим маршрутизатором. Побудуємо мережу (рис.23.8).

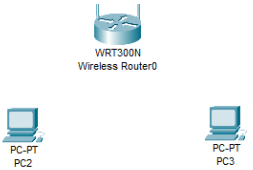

Рис. 23.8. Зв'язок між *Laptop2* та *Laptop3*

Якщо додати на обидва *PC* бездротові модулі *WPN300N*, то зв'язок з маршрутизатором відразу встановиться. Зайдемо на маршрутизаторі і налаштуємо автентифікацію (рис.23.9).

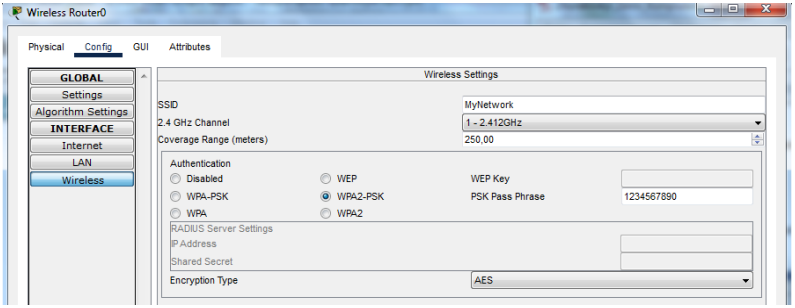

Рис. 23.9. Налаштування маршрутизатора

Зв'язок між маршрутизатором і *PC* зник. На *PC2* заходимо в меню *PC Wireless*, вкладка *Connect*. Вибираємо мережу *MyNetwork*, натискаємо на *Connect*, вводимо Pre-*shared Key* 1234567890, потім знову *Connect*. Аналогічні налаштування робимо і для *PC3*. В результаті *PC* під'єднуються до маршрутизатора (рис. 23.10). *IP*-адреси на *PC* проставляються динамічно від маршрутизатора.

Рис. 23.10. Зв'язок *PC* та маршрутизатора

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл.23.1.

Таблиця 23.1

Завдання

Номер варіанта	Мережа до рис.23.1	Мережа до рис.23.2	Мережа до рис.23.3	*ssid* до рис.23.4
1	10.10.10.0	10.10.10.0, 1.1.1.0	1.1.1.0, 1.1.2.0, 1.1.3.0	*network1*
2	10.10.20.0	10.10.20.0, 1.1.2.0	1.1.2.0, 1.1.3.0, 1.1.4.0	*network2*
3	10.10.30.0	10.10.30.0, 1.1.3.0	1.1.3.0, 1.1.4.0, 1.1.5.0	*network3*
4	10.10.40.0	10.10.40.0, 1.1.4.0	1.1.4.0, 1.1.5.0, 1.1.6.0	*network4*
5	10.10.50.0	10.10.50.0, 1.1.5.0	1.1.5.0, 1.1.6.0, 1.1.7.0	*network5*
6	10.10.60.0	10.10.60.0, 1.1.6.0	1.1.6.0, 1.1.7.0, 1.1.8.0	*network6*
7	10.10.70.0	10.10.70.0, 1.1.7.0	1.1.7.0, 1.1.8.0, 1.1.9.0	*network7*
8	10.10.80.0	10.10.80.0, 1.1.8.0	1.1.8.0, 1.1.9.0, 1.1.1.0	*network8*
9	10.10.90.0	10.10.90.0, 1.1.9.0	1.1.9.0, 1.1.1.0, 1.1.2.0	*network9*
10	10.10.100.0	10.10.100.0, 1.1.10.0	1.1.1.0, 1.1.3.0, 1.1.4.0	network10

4. До схеми на рис. 23.1 додати ще один *PC* та налаштувати бездротову мережу *WEP* відповідно до варіанта.

5. До схеми на рис. 23.4 додати два *PC* та налаштувати бездротову мережу з використанням *WPA*.

6. До схеми на рис. 23.6 додати ще одну точку доступу та *Laptop*, налаштувати бездротову мережу.

7. До схеми на рис. 23.8 додати три *PC* та налаштувати бездротову мережу.

8. Оформити звіт за результатами виконаної роботи.

Запитання та завдання для самоперевірки

1. Що таке бездротова мережа?
2. На основі якого стандарту працюють бездротові мережі?
3. Що таке *Wi-Fi*?
4. Поясніть призначення адаптера.
5. Для чого використовується ключ безпеки?
6. Які ви знаєте типи шифрування *Wi-Fi*?
7. Як налаштувати мережу із застосуванням *WPA*?
8. Що таке *SSID*?
9. Як налаштувати мережу із застосуванням *WEP*?
10. Що таке точка доступу та як її налаштувати?

Лабораторна робота 24
НАЛАШТУВАННЯ IPV6-АДРЕС НА МЕРЕЖНИХ ПРИСТРОЯХ

Мета: ознайомитися принципами *IP*-адресації версії 6, налаштувати IPv6-адресацію на мережних пристроях в *Cisco Packet Tracer*.

Основні теоретичні відомості

IP-адреса версії 6 має довжину 128 бітів (16 байтів). Запис такої адреси здійснюється у шістнадцятковій формі числення як вісім груп по 16 бітів (два байти), як роздільник груп застосовується двокрапка.

Діапазон можливих *IP*-адрес версії 6 містить 2^{128} *IP*-адрес і має вигляд:

0000:0000:0000:0000:0000:0000:0000:0000 –
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

На практиці застосовуються повна і спрощена форми запису *IP*-адрес версії 6. Повна форма передбачає запис усіх цифр *IP*-адреси. Спрощена форма дозволяє не записувати ведучі нулі у групах та замінювати одну з послідовностей нульових груп записом «::».

Приклад повної форми запису *IPv6*:

2001:0DB8:0000:0000:0000:FF00:0042:8329.

Приклад частково спрощеної форми запису *IPv6*:

2001:DB8:0:0:0:FF00:42:8329.

Приклад спрощеної форми запису *IPv6*:

2001:DB8::FF00:42:8329.

Як і для *IP*-адрес версії 4, деякі адреси з діапазону *IPv6* зарезервовані для спеціального використання. Повний перелік та опис спеціалізованих *IP*-адрес версії 6 міститься у стандарті *RFC*-6890. Основні з них наведені у табл. 24.1.

Таблиця 24.1

Основні спеціальні *IPv6* –адреси та їх призначення

IPv6-адреса	Назва	Застосування
:: /128	Невизначена *IPv6*-адреса (*Unknown IPv6-Address*)	Позначення поточного вузла. Адреса відправника повідомлення у випадку, коли вузол не має адресної інформації
::1 /128	*IPv6*-адреса зворотної петлі (*Loopback*, *Localhost IPv6-Address*)	Тестування роботи стека *TCP*/IP, а також організація роботи клієнтської і серверної частин додатка, які функціонують на одному вузлі
FE80::/10	*IPv6*-адреса локального використання (*Linked-Scoped Unicast IPv6-Address*)	Адреса локального використання. Формується на основі *MAC*-адреси вузла. Номер мережі – *FE80*::
FFxx:: /8	*IPv6*-групова адреса (*IPv6 Multicast Address*)	Групова *IPv6*-адреса

Залежно від застосування *IPv6*-адреса може бути ідентифікована як:

– унікальна *IPv6*-адреса (*Unicast IPv6-Address*);

– групова *IPv6*-адреса (*Multicast IPv6-Address*);

– *IPv6*-адреса одного з групи (*Anycast IPv6-Address*).

У повідомленні (*IPv6*-пакеті) унікальні *IPv6*-адреси можуть зазначатися і як адреси відправника (Source *IPv6-Address*), і як адреси

отримувача (*Destination IPv6-Address*). Групові *IPv6*-адреси і *IPv6*-адреси одного з групи можуть зазначатися лише як адреси отримувача. *IP*-адреса отримувача визначає, яким є *IP*-пакет: унікальним, груповим тощо. Для широкомовної розсилки в *IP* версії 6 застосовуються групові *IPv6*-адреси.

Структурно *IP*-адреса версії 6 складається з двох однакових за довжиною частин – одна частина (64 біти ліворуч) містить *IP*-адресу (номер) мережі, до якої належить вузол, інша (64 біти праворуч) – *IP*-адресу (номер) вузла в цій мережі. Відокремлення номера мережі від номера вузла здійснюється за допомогою префікса мережі /64. Особливістю *IP*-адреси версії 6 є те, що номер мережі містить у собі номери багатьох підмереж. Відповідно застосовується кілька префіксів підмереж.

Перелік типових *IPv6* префіксів підмереж наведено у табл. 24.2.

Таблиця 24.2

Типові IPv6 –префікси

префікс	*IPv6*-адреса	префікс	*IPv6*-адреса
/4		/36	Виділено для майбутнього використання для *LIR* надмалого розміру
/8		/40	
/12	Виділено *IANA* для *RIR*	/44	
/16		/48	Призначається великим сайтам та провайдерам
/20	Виділено для *LIR* дуже великого розміру	/52	
/24	Виділено для LIR великого розміру	/56	Призначається кінцевим сайтам (домашнім мережам)
/28	Виділено для *LIR* середнього розміру	/60	Обмежене використання
/32	Виділено для *LIR* малого розміру	/64	Одна локальна мережа (типовий префікс для *SLAAC*)

Розглянемо налаштування *IPv6*-адрес на мережних пристроях на прикладі схеми (рис. 24.1).

Для встановлення з'єднання між маршрутизаторами *R1* та *R2*, для обох маршрутизаторів необхідно додати модуль *HWIC*-2T. В режимі глобальної конфігурації активуємо *IPv6*-маршрутизацію на маршрутизаторі *R1*:

R1(config)# ipv6 unicast-routing

Присвоїмо мережним інтерфейсам маршрутизатора *IPv6*-адреси.

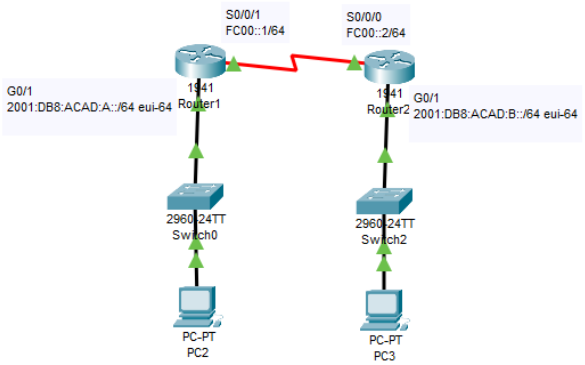

Рис. 24.1. Схема мережі

Інтерфейс *G0*/1 має глобальну маршрутизовану індивідуальну адресу, *EUI*-64 використовується для створення ідентифікатора в адресі. Інтерфейс *S0/0/1* має локально-маршрутизовану унікальну локальну адресу, який рекомендується використовувати для послідовних з'єднань типу точка-точка:

Router(config)#ipv6 unicast-routing
Router(config)#interface g0/1
Router(config-if)#ipv6 address 2001:DB8:ACAD:A::/64 eui-64
Router(config-if)#no shutdown
Router(config-if)#interface serial 0/0/1
Router(config-if)#ipv6 address FC00::1/64
Router(config-if)#no shutdown

Аналогічні налаштування введемо і для маршрутизатора *R2*:

Router(config)#ipv6 unicast-routing
Router(config)#interface gigabit 0/1
Router(config-if)#ipv6 address 2001:DB8:ACAD:B::/64 eui-64
Router(config-if)#no shutdown
Router(config-if)#interface serial 0/0/0
Router(config-if)#ipv6 address FC00::2/64
Router(config-if)#clock rate 128000
Router(config-if)#no shutdown

Для *PC2* та *PC3* включіть автоматичне отримання *IPv6*-адреси. Після цього *PC* зв'яжуться з маршрутизаторами для отримання

даних про підмережу та шлюз та автоматично налаштують свої *IPv6*-адреси. Далі налаштуємо статичний маршрут *IPv6* на обох маршрутизаторах:

Router1(config)#ipv6 route 2001:DB8:ACAD:B::/64 FC00::2

Router2(config)#ipv6 route 2001:DB8:ACAD:A::/64 FC00::1

Для тестування працездатності мережі відправимо з *PC3* на *PC1* ping-запит. Як видно з рис. 24.2, всі пакети отримані.

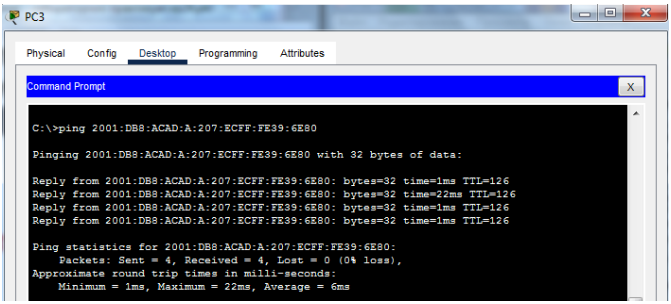

Рис. 24.2. тестування працездатності мережі

Завдання до виконання лабораторної роботи

У ході лабораторної роботи необхідно виконати наступні дії:

1. Вивчити теоретичну частину лабораторної роботи.
2. Ознайомитися з довідковою літературою.
3. Вибрати варіант в табл. 24.3, побудувати мережу (рис. 24.3), налаштувати *IPv6*-маршрутизацію – для маршрутизаторів статичну відповідно до варіанта завдання, для комп'ютерів – автоматичну.

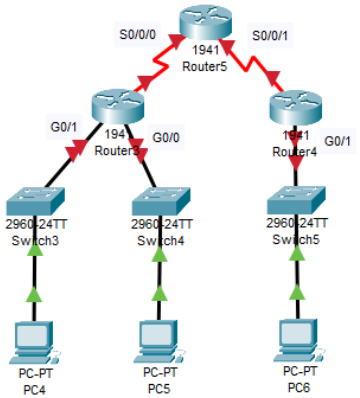

Рис. 24.3. Схема мережі до завдання

4. Перевірити працездатність мережі ping-запитом між PC.
5. Оформити звіт за результатами виконаної роботи.

Таблиця 24.1

Завдання

Номер варіанта	*R3* *G0/0, G0/1*	*R4* *G0/1*	*R5* *S0/0/0, S0/0/1*
	2001:DB8:ACAD:B::: *2001:DB8:ACAD:A:::*	*001:DB8:CAFE:1::1*	*2001:DB8:AAAA:1:::* *2001:DB8:AAAA:2:::*
1	*2001:DB8:ACAD:A:::* *2001:DB8:ACAD:B:::*	*001:DB8:CAFE:2::1*	*2001:DB8:AAAA:3:::* *2001:DB8:AAAA:4:::*
2	*2001:DB8:ACAD:B:::* *2001:DB8:ACAD:A:::*	*001:DB8:CAFE:3::1*	*2001:DB8:AAAA:5:::* *2001:DB8:AAAA:6:::*
3	*2001:DB8:ACAD:A:::* *2001:DB8:ACAD:B:::*	*001:DB8:CAFE:4::1*	*2001:DB8:AAAA:7:::* *2001:DB8:AAAA:8:::*
4	*2001:DB8:ACAD:B:::* *2001:DB8:ACAD:A:::*	*001:DB8:CAFE:5::1*	*2001:DB8:AAAA:1:::* *2001:DB8:AAAA:2:::*
5	*2001:DB8:ACAD:A:::* *2001:DB8:ACAD:B:::*	*001:DB8:CAFE:6::1*	*2001:DB8:AAAA:3:::* *2001:DB8:AAAA:4:::*
6	*2001:DB8:ACAD:B:::* *2001:DB8:ACAD:A:::*	*001:DB8:CAFE:7::1*	*2001:DB8:AAAA:5:::* *2001:DB8:AAAA:6:::*
7	*2001:DB8:ACAD:A:::* *2001:DB8:ACAD:B:::*	*001:DB8:CAFE:8::1*	*2001:DB8:AAAA:7:::* *2001:DB8:AAAA:8:::*
8	*2001:DB8:ACAD:B:::* *2001:DB8:ACAD:A:::*	*001:DB8:CAFE:9::1*	*2001:DB8:AAAA:1:::* *2001:DB8:AAAA:2:::*
9	*2001:DB8:ACAD:A:::* *2001:DB8:ACAD:B:::*	*001:DB8:CAFE:A::1*	*2001:DB8:AAAA:3:::* *2001:DB8:AAAA:4:::*
10	*2001:DB8:ACAD:B:::* *2001:DB8:ACAD:A:::*	*001:DB8:CAFE:B::1*	*2001:DB8:AAAA:5:::* *2001:DB8:AAAA:6:::*

Запитання та завдання для самоперевірки

1. Який формат має адреса *IPv6*?
2. Як визначити розмір адресного простору *IPv6*?
3. Порівняйте формат адреси *IPv4* та *IPv6*.
4. Який синтаксис запису *IPv6*?
5. Які області адрес *IPv6*?
6. Назвіть типи *IPv6*-адрес та охарактеризуйте їх.
7. Які типи *IPv6*-адрес на інтерфейсах є обов’язковими?
8. Наведіть приклади префіксів та їх призначення.
9. Наведіть приклади відомих групових *IPv6*-адрес.

Список джерел

1. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2001. -672 с.
2. Комп'ютерні мережі. Частина 2.// Навчальний посібник / І. Р. Арсенюк, А. А. Яровий. – Вінниця: ВНТУ, 2011. – 145 с.
3. Комп'ютерні мережі. Частина 3.// Навчальний посібник / І. Р. Арсенюк, А. А. Яровий. – Вінниця: ВНТУ, 2017. – 85 с.
4. Комп'ютерні мережі та технології: навч. посібник для студ. вищих навч. закл. / І. А. Жуков [и др.]. – К. : НАУ, 2004. – 276 с.
5. Комп'ютерні мережі // навчальний посібник з грифом МОН України / Ю.О. Кулаков, І.А. Жуков. – «НАУ-друк», 2009. – 329 с.
6. Моделирование компьютерных сетей: Учебное пособие / С.В. Бейцун, М.В. Кулинич. – Днепропетровск: НМетАУ, 2016. – 96 с.
7. Телекомунікаційні та інформаційні мережі: Підручник (для вищих навчальних закладів) / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.
8. Компютерні мережі. [2-е вид., оновл. і доповн.] / Є. Буров. – Львів : БаК, 2–3. – 584 с.
9. TCP/IP для профессионалов. 3-е изд./ Т. Паркер, К. Синян. - СПб.: Питер, 2004. -859 с.
10. Пособие для самостоятельного изучения. Маршрутизаторы Cisco. – Пер. с англ. / Д. Ф. Димарцио. – СПб: СимволПлюс, 2003. – 512 с.
11. TCP/IP. Сетевое администрирование, 3-е издание- Пер. с англ. / Крэйг Хант – СПб: Символ-Плюс, 2007. - 816 с.
12. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200101: маршрутизация и коммутация, акад. изд.: Пер. с англ. / Одом, Уэнделл. – М .: ООО "И.Д. Вильяме", 2015. – 736 с.

Навчальне видання

КОМП’ЮТЕРНІ МЕРЕЖІ

Лабораторний практикум
для студентів спеціальності 123
«Комп’ютерна інженерія»

Укладачі:
ПРОЦЕНКО Микола Михайлович
ПАЩЕНКО Наталія Вікторівна